Office for Nuclear Regulation

An agency of HSE

Generic Design Assessment – New Civil Reactor Build

Step 4 Control and Instrumentation Assessment of the EDF and AREVA UK EPR™ Reactor

Assessment Report: ONR-GDA-AR-11-022
Revision 0
11 November 2011

COPYRIGHT

First published December 2011

PREFACE

The Office for Nuclear Regulation (ONR) was created on 1st April 2011 as an Agency of the Health and Safety Executive (HSE). It was formed from HSE's Nuclear Directorate (ND) and has the same role. Any references in this document to the Nuclear Directorate (ND) or the Nuclear Installations Inspectorate (NII) should be taken as references to ONR.

The assessments supporting this report, undertaken as part of our Generic Design Assessment (GDA) process and the submissions made by EDF and AREVA relating to the UK EPR™ reactor design, were established prior to the events at Fukushima, Japan. Therefore, this report makes no reference to Fukushima in any of its findings or conclusions. However, ONR has raised a GDA Issue which requires EDF and AREVA to demonstrate how they will be taking account of the lessons learnt from the events at Fukushima, including those lessons and recommendations that are identified in the ONR Chief Inspector's interim and final reports. The details of this GDA Issue can be found on the Joint Regulators' new build website www.hse.gov.uk/newreactors and in ONR's Step 4 Cross-cutting Topics Assessment of the EDF and AREVA UK EPR™ reactor.

EXECUTIVE SUMMARY

My report presents the findings of the Control and Instrumentation (C&I) assessment of the UK EPR reactor undertaken as part of Step 4 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA). I carried out my assessment using the Pre-Construction Safety Report (PCSR) and supporting documentation submitted by EDF and AREVA during GDA Step 4.

My assessment has followed a step-wise-approach in a claims-argument-evidence hierarchy. In GDA Step 2, the claims made by EDF and AREVA (the Requesting Party (RP)) were examined; in GDA Step 3 the arguments that underpin those claims were examined.

The scope of the GDA Step 4 assessment was to review the safety aspects of the UK EPR reactor in greater detail, by examining the evidence, supporting arguments and claims made in the safety documentation. The GDA Step 4 assessment builds on the assessments already carried out for GDA Steps 2 and 3, and provides a judgement on the adequacy of the C&I information contained within the PCSR and supporting documentation.

It is seldom possible, or necessary, to assess a safety case in its entirety; therefore, sampling is used to limit the areas scrutinised, and to improve the overall efficiency of the assessment process. Sampling is performed in a focused, targeted and structured manner with a view to revealing any topic-specific or generic weaknesses in the safety case. To identify the sampling for the C&I an assessment plan for GDA Step 4 was set-out in advance.

My assessment has focussed on the:

- arguments and evidence presented for conformance to the HSE C&I Safety Assessment Principles (SAPs);
- principal design and implementation standards for all C&I safety and safety related systems (i.e. the Systems Important to Safety (SIS));
- RP's safety case for selected key C&I SIS and platforms used to implement the systems (e.g. covering the safety Class 1 Protection System (PS), Class 2 Safety Automation System (SAS) and Class 3 Process Automation System (PAS));
- C&I architecture including provision for defence-in-depth, independence and diversity (including review of EDF and AREVA's responses to Regulatory Issue (RI) RI-UKEPR-002 raised on the adequacy of the UK EPR C&I architecture); and
- diversity of those systems contributing to implementation of the highest category safety functions (e.g. PS and SAS / PAS).

A number of items have been agreed with EDF and AREVA as being outside the scope of the GDA process and hence have not been included in my assessment.

From my assessment, I have concluded that the:

- PCSR and supporting documentation cover the main C&I SIS expected in a modern nuclear reactor;
- principal design and implementation standards used by EDF and AREVA for all C&I SIS are broadly in accordance with those expected in the nuclear sector;
- RP's safety case for the sampled key C&I SIS and platforms used to implement the SIS is broadly in line with expectations; and
- significant C&I architecture concerns raised in RI RI-UKEPR-002 have been addressed by i) the reduction of reliability claims for the computer-based SIS, and ii) introduction of a

safety Class 2 Non-Computerised Safety System (NCSS), one way network communication from the PS to lower classified systems, and Class 1 displays and manual controls.

In some areas there has been a lack of detailed information which has limited the extent of my assessment. As a result I will need additional information to underpin my conclusions, and these are identified as Assessment Findings to be carried forward as normal regulatory business. Assessment Findings have been raised to cover items such as standards' compliance demonstration, and implementation of process improvements (e.g. relating to PS requirements traceability and production of method statements). Assessment Findings are listed in Annex 1.

Some of the observations identified within this report are of particular significance and will require resolution before HSE would agree to the commencement of nuclear safety related construction of a UK EPR reactor in the UK. These are identified in this report as GDA Issues and are listed in Annex 2. In summary, these relate to:

- revision of the safety case to address the introduction of the NCSS, including the demonstration of its diversity from the computer-based safety systems;
- revision of the safety case to address PS changes to ensure there are only outward network communications to other systems from the PS, and justification of the small number of hardwired links to the PS;
- justification of the revised reliability figures used for the protection systems (PS, SAS / PAS and NCSS) when claimed independently and in combination;
- provision of detailed substantiation of the Class 1 control and display facilities, including justification of functional coverage;
- revision of the safety case to classify the C&I systems (e.g. PAS and SAS) in accordance with international standards and commitments provided by EDF and AREVA;
- finalisation of the PS independent confidence building activities' scope (covering statistical testing, static analysis and compiler validation), and definition of production excellence and independent confidence building measures for other SIS;
- enhancements to the safety case, in particular, to the presentation of the claims-arguments-evidence trail (i.e. covering key safety case claims and SAP conformance);
- fully defining the approach to the justification of smart devices (based on computer technology) used in SIS, including provision of a programme showing when implementation evidence will be available; and
- revision of the SAS / PAS safety case to address obsolescence of the SPPA-T2000 (Siemens S5 based) platform.

Overall, based on the sample undertaken in accordance with ND procedures, I am broadly satisfied that the claims, arguments and evidence laid down within the PCSR and supporting documentation submitted as part of the GDA process present an adequate safety case for the generic UK EPR reactor design. The UK EPR reactor is therefore suitable for construction in the UK with respect to the adequacy of C&I, subject to satisfactory progression and resolution of GDA Issues to be addressed during the forward programme for this reactor and assessment of additional information that becomes available as the GDA Design Reference is supplemented with additional details on a site-by-site basis.

LIST OF ABBREVIATIONS

ASIC	Application Specific Integrated Circuits
ASN	Autorité Sûreté Nucléaire – French Nuclear Safety Authority
BMS	(Nuclear Directorate) Business Management System
BSC	Basis of Safety Case
C&I	Control and Instrumentation
CAE	Claims-Argument-Evidence
CBSIS	Computer Based Systems Important to Safety
CCF	Common Cause Failure
CPLD	Complex Programmable Logic Devices
DAC	Design Acceptance Confirmation
EDF and AREVA	Electricité de France SA and AREVA
FA3	Flamanville 3 Nuclear Power Plant
FPGA	Field Programmable Gate Array
FMEA	Failure Modes and Effects Analysis
GDA	Generic Design Assessment
HMI	Human Machine Interface
HSE	Health and Safety Executive
ICBM	Independent Confidence Building Measures
iDAC	Interim Design Acceptance Confirmation
IEC	International Electrotechnical Commission
IAEA	International Atomic Energy Agency
MCR	Main Control Room
MDEP	Multinational Design Evaluation Programme
NC	Non-Categorised
NCSS	Non-Computerised Safety System
ND	The (HSE) Nuclear Directorate
NEA	Nuclear Energy Agency
NP	Nuclear Plant
OECD	Organisation for Economic Co-operation and Development
PACS	Priority Actuation Control System
PAS	Process Automation System
PCEC	Programmable Complex Electronic Components
PCSR	Pre-Construction Safety Report
PICS	Process Information and Control System
PIE	Postulated Initiating Events
PIPS	Process Instrumentation Preprocessing System

LIST OF ABBREVIATIONS

pfd	Probability of Failure on Demand
PS	Protection System
PSA	Probabilistic Safety Analysis
QDS	Qualified Display System
QMS	Quality Management System
RCSL	Reactor Control, Surveillance and Limitation system
RI	Regulatory Issue
RO	Regulatory Observation
RP	Requesting Party
RPMS	Rod Position and Monitoring System
RRC-B	Risk Reduction Category - B
RSS	Remote Shutdown Station
SAP	HSE Nuclear Directorate Safety Assessment Principle
SAS	Safety Automation System
SCC	Source to Code Comparison
SICS	Safety Information and Control System
SIS	Systems Important to Safety
SIVAT	Simulation Based Validation Tool
SRS	Safety Related Systems
SS	Safety Systems
STUK	Sateilyturvakeskus, the Finnish regulator
TAG	(Nuclear Directorate) Technical Assessment Guide
TO	TSC Technical Observation
TQ	Technical Query
TSC	Technical Support Contractor
TXS	Teleperm XS
US	United States
US NRC	US Nuclear Regulatory Commission

TABLE OF CONTENTS

1 INTRODUCTION 1
2 NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR C&I 2
2.1 Assessment Plan 2
2.2 Standards and Criteria 3
2.3 Assessment Scope 3
2.3.1 Findings from GDA Step 3 4
2.3.2 Additional Areas for Step 4 C&I Assessment 4
2.3.3 Use of Technical Support Contractors 4
2.3.4 Cross-cutting Topics 5
2.3.5 Out of Scope Items 6
3 REQUESTING PARTY'S SAFETY CASE 9
4 GDA STEP 4 NUCLEAR DIRECTORATE ASSESSMENT FOR C&I 10
4.1 Step 4 C&I SAP and Safety Case Claims-Arguments-Evidence Assessment 10
4.1.1 Assessment 10
4.1.2 Findings 13
4.2 C&I Systems' Classification and Standards 13
4.2.1 Assessment 13
4.2.2 Findings 17
4.3 C&I SIS Platforms and Pre-Developed Equipment 18
4.3.1 Assessment 18
4.3.2 Findings 27
4.4 C&I Systems Important to Safety 28
4.4.1 Assessment 28
4.4.2 Findings 38
4.5 C&I System Level Architecture 39
4.5.1 Assessment 39
4.5.2 Findings 44
4.6 Diversity of Systems Implementing Reactor Protection Functionality 44
4.6.1 Assessment 44
4.6.2 Findings 46
4.7 Overseas Regulatory Interface 46
4.7.1 Bilateral Collaboration 46
4.7.2 Multilateral Collaboration 47
5 CONCLUSIONS 48
5.1 Key Findings from the Step 4 Assessment 48
5.1.1 Assessment Findings 49
5.1.2 GDA Issues 49
6 REFERENCES 50

Tables

Table 1: C&I Scope: C&I Automation Systems
Table 2: C&I Scope: Instrumentation
Table 3: C&I Scope: C&I Platform Development
Table 4: C&I Scope: HMI Systems
Table 5: Relevant Safety Assessment Principles for Control & Instrumentation Considered During Step 4

Annexes

Annex 1: Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business - Control & Instrumentation – UK EPR
Annex 2: GDA Issues – Control & Instrumentation – UK EPR
Annex 3: TSC Task Summary – C&I SAP Conformance and Adequacy of PCSR Review for UKEPR
Annex 4: TSC Task Summary - Review of EDF/AREVA QMS Processes Against Principal Design and Implementation Standards Report
Annex 5: TSC Task Summary - Review of Class 1 and 2 System Platforms and Pre-Developed Components Report
Annex 6: TSC Task Summary - Review of C&I Safety and Safety-Related Systems
Annex 7: TSC Task Summary - Review of the C&I Architecture for Safety Capability
Annex 8: TSC Task Summary - Review of the Diversity of those Systems Contributing to the Implementation of Category A Functions
Annex 9: TSC Task Summary - Review of Responses to Regulatory Issue RI-UKEPR-002

1 INTRODUCTION

1 My report presents the findings of the GDA Step 4 Control and Instrumentation (C&I) assessment of the UK EPR reactor Pre-Construction Safety Report (PCSR) (Ref. 22) and supporting documentation provided by EDF and AREVA under the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process. Assessment was undertaken of the PCSR and the supporting evidentiary information derived from the Master Submission List (Ref. 23). The approach taken was to assess the main submission, i.e. the PCSR, and then undertake assessment of the relevant documentation sourced from the Master Submission List on a sampling basis in accordance with the requirements of ND Business Management System (BMS) procedure AST/001 (Ref. 2). I used the Safety Assessment Principles (SAPs) (Ref. 4) as the basis for this assessment. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

2 During the assessment a number of Technical Queries (TQs), topic meeting actions, Regulatory Observations (ROs) and one Regulatory Issue (RI) were issued and the responses made by EDF and AREVA assessed. Where relevant, detailed design information from specific projects for this reactor type has been assessed to build confidence and assist in forming a view as to whether the design intent proposed within the GDA process can be realised.

3 It is not the purpose of this report to provide a detailed description of the C&I architecture; such description may be found in “PCSR – Sub-Chapter 7.2 – General architecture of the Instrumentation & Control systems” (Ref. 22).

4 A number of items have been agreed with EDF and AREVA as being outside the scope of the GDA process and hence have not been included in this assessment. These are identified in Section 2.3.5 of this report.

2 NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR C&I

5 My GDA Step 4 assessment strategy for the C&I topic area was set out in an assessment plan (Ref. 1) that identified the intended scope of the assessment and the standards and criteria that would be applied. This is summarised below.

2.1 Assessment Plan

6 The objective of the GDA Step 4 C&I assessment was to review the safety aspects of the proposed C&I design by examining the evidence supporting the claims and arguments made in EDF and AREVA's safety documentation. The GDA Step 4 assessment builds on the GDA Steps 2 and 3 work, and provides a judgement on the adequacy of the C&I safety demonstration contained within the PCSR and supporting documentation.

7 My GDA Step 4 assessment examined the remaining claims not previously assessed (e.g. addressing relevant HSE SAPs not previously considered) and the underpinning arguments. However, the scope of this assessment was primarily concerned with examination of samples of the 'evidence' to support claims for all HSE SAPs within the scope of assessment. For C&I 'evidence' was broadly interpreted as including:

- the detailed documentation showing conformance with the relevant HSE SAPs (i.e. how the HSE SAP goals are met);
- the detailed documentation showing compliance with the standards for the equipment, production processes and safety justification;
- information substantiating the C&I functionality and reliability claims; and
- information supporting production excellence for the pre-existing platforms.

8 My GDA Step 4 assessment included a review of the processes to be used to produce and justify the application specific software and hardware for the Safety Systems (SS) and Safety Related Systems (SRS) (i.e. the Systems Important to Safety (SIS)). Samples of the application software (using examples from the Flamanville 3 (FA3) plant) were reviewed.

9 My GDA Step 4 assessment commenced with consideration of the relevant chapters of the PCSR and supporting references available at that time, and these are referred to as appropriate in this report. As the GDA submission developed during Step 4, in response to my regulatory questions, amendments were made as appropriate to the PCSR and its supporting references.

10 I reviewed the updates to the C&I GDA submission and determined that the updates to or information included in the GDA submission and/or supporting references were not as expected. Further work is required to address these shortfalls. This will be progressed in GDA through a C&I GDA Issue **GI-UKEPR-CI-03** and cross-cutting GDA Issue **GI-UKEPR-CC-02**. In the C&I topic area my assessment is therefore limited to the versions of the GDA submission documents referred to in my Assessment Report. Although the consolidated PCSR (Ref. 62) and its supporting references are therefore acceptable as the reference point for an Interim Design Acceptance Confirmation (iDAC) the outstanding GDA Issues require acceptable resolution before a final Design Acceptance Confirmation (DAC) can be issued.

2.2 Standards and Criteria

11 The standards and criteria that were used to judge the adequacy of the UK EPR C&I were HSE SAPs (Ref. 4), Technical Assessment Guides (TAGs) and relevant international standards and guidance (e.g. Ref. 5). Table 5 identifies the HSE C&I SAPs considered during my assessment.

12 Nuclear Directorate's (ND's) C&I TAGs provide further guidance for some of the HSE C&I SAPs. The key TAGs are T/AST/003 (Ref. 8) for SS and T/AST/046 (Ref. 9) for systems containing computer / complex technology. The majority of the SIS deployed on the UK EPR contain such technology.

13 The standards and criteria used for the C&I GDA Step 4 assessment included relevant nuclear sector standards related to SIS design (e.g. BS IEC 61513:2001 (Ref. 10) and BS IEC 62340:2007 (Ref. 11)). Other significant guidance includes the report of the seven party task force on safety critical software (Ref. 5).

2.3 Assessment Scope

14 The C&I GDA Step 4 assessment included the specific elements shown below.

- Completion of the technical review of EDF and AREVA's responses to regulatory issue RI-UKEPR-002 and resolution of ND GDA Step 3 Assessment Report observations (Ref. 6). For example, covering topics such as categorisation of functions, classification of systems, compliance to International Electrotechnical Commission (IEC) C&I SIS standards and the special case procedure for computer-based systems (Ref. 9).
- Review of the "arguments" and "evidence" made for conformance to the HSE C&I SAPs (Ref. 4) (i.e. completion of the claims-arguments-evidence (CAE) based review against the SAPs).
- Review of the principal design and implementation standards for C&I SIS (Class 1, 2 and 3) equipment. Sampling of detailed evidence during GDA Step 4 (e.g. to demonstrate the standards have been adequately applied) predominately focused on the Class 1 systems (e.g. reactor protection) and the key Class 2 SIS.
- Review of EDF and AREVA's safety case for the Class 1 (e.g. Teleperm XS (TXS)) and key Class 2 SIS platforms and pre-developed components using appropriate guidance and standards.
- Review of the safety case for the implementation of the Class 1 and key Class 2 SIS (e.g. development of application code, independent verification and validation, and independent confidence building measures) using the platforms and pre-developed equipment selected by EDF and AREVA.
- Further review of the C&I architecture including provisions for defence-in-depth, independence and diversity, automatic and manual safety actuations, and appropriateness of equipment class.
- Further review of the diversity of those systems contributing to implementation of Category A functions (e.g. Protection System (PS) and Safety Automation System (SAS)).
- Review of the impact of PCSR revisions.

2.3.1 Findings from GDA Step 3

15 The findings of my GDA Step 3 Assessment Report (Ref. 6) are summarised below.

- A number of significant concerns (raised in RI-UKEPR-002) were identified in relation to the adequacy of the UK EPR architecture, namely:
  - i) substantiation of the reliability claims for the computer-based SIS (CBSIS) that use the TXS and SPPA-T2000 platforms;
  - ii) complexity and interconnectivity of the architecture, and independence of systems;
  - iii) absence of Class 1 displays and manual controls.
- The PCSR and supporting documentation cover the main C&I systems and provisions that would be expected in a modern nuclear reactor but the safety case argumentation and identification of evidence needed improvement.

16 EDF and AREVA proposed a way forward in relation to RI-UKEPR-002 that provided a basis for proceeding to GDA Step 4, which included:

- provision of a backup safety system that is not based on computer technology and is known as the Non-Computerised Safety System (NCSS);
- one-way network communication from the Protection System (PS) to lower classified systems; and
- the provision of a Class 1 display facility and manual controls.

In addition to changes in the technology and C&I architecture, EDF and AREVA also agreed to a reduction of the CBSIS reliability claims. Assessment of these proposals and EDF and AREVA's response to concerns raised in the GDA Step 3 Assessment Report (Ref. 6) is provided in Section 4.

2.3.2 Additional Areas for Step 4 C&I Assessment

17 My GDA Step 4 assessment includes completion of the review of HSE C&I SAPs considered appropriate for sampling during assessment of a new reactor design. Therefore, there is an increase in the number of HSE SAPs reviewed during GDA Step 4 compared to that assessed during GDA Step 3. In addition, GDA Step 4 included sampling of the detailed evidence used to substantiate safety case claims.

18 During GDA Step 4 the assessment scope was widened to include coverage of the C&I standards for Class 1, 2 and 3 SIS, a review of key C&I platforms (e.g. TXS and SPPA-T2000) and a review of the processes used to develop applications for systems using these platforms.

2.3.3 Use of Technical Support Contractors

19 A Technical Support Contractor (TSC) was engaged to assist with the C&I assessment work in GDA Step 3, and the same contractor assisted during GDA Step 4. The scope of work undertaken by the TSC included:

- sample-based review of the evidence used to demonstrate conformance to HSE C&I SAPs;

- sample-based review of the main design and implementation standards used for C&I SIS related equipment (i.e. for architecture, platforms (TXS and SPPA-T2000), applications, and also smart devices);
- sampling of the detailed design and implementation evidence of the Class 1 platform (TXS) and the Class 2 platform (SPPA-T2000);
- sampling of the detailed evidence of the implementation methods for Class 1 systems (e.g. PS), Class 2 systems (e.g. SAS) and Class 3 systems (e.g. PAS);
- sampling of the detailed evidence of C&I architecture safety capability, including a review of the overall system integration; and
- sampling of the detailed evidence of the diversity of the designs of platforms and systems contributing to implementation of Category A functions, and assessment of the possible contribution of platforms / systems to Common Cause Failure (CCF) of the Category A functions.

20 The TSC undertook detailed technical reviews under the close direction and supervision of ND. The regulatory judgment on the adequacy or otherwise of the UK EPR C&I was made exclusively by ND. All ROs, TQs and the one RI were raised by ND.

21 The TSC has provided GDA Step 4 reports that address the scope of work listed above. The TSC also reviewed responses to ROs, TQs and Level 3 meeting Actions placed on EDF and AREVA. The TSC reports include a summary statement of the results of its work and findings (i.e. Technical Observations (TOs)). The summary statements including all TOs are reproduced in Annexes 3 to 9 of this report. I have reviewed the TSC's TOs and, as considered appropriate, taken them forward under GDA Issues (see Annex 2) or Assessment Findings (see Annex 1). The TSC TOs provide further guidance on the GDA Issues or Assessment Findings and their means of resolution. Within this report, references to the TSC TOs are provided using the unique TO identifiers (e.g. T17.TO1.01).

2.3.4 Cross-cutting Topics

22 I address the following Cross-cutting Topics in this report: Safety Categorisation and Classification, and Smart Devices.

23 Safety Categorisation and Classification - The four levels of functional categorisation (F1A, F1B, F2 and Non-Categorised (NC)) and C&I system classification (E1A, E1B, E2 and NC) proposed by EDF and AREVA do not align with HSE's SAPs (Ref. 4) or relevant British issue of international C&I standards (i.e. BS IEC 61513 (Ref. 10) and BS IEC 61226:2005 (Ref. 13)). This concern was initially raised with EDF and AREVA as part of RI-UKEPR-002 (Ref. 26) and then progressed as a transverse issue (i.e. affecting more than one topic area) as part of RO-UKEPR-43. EDF and AREVA have stated that categorisation and classification will be in accordance with BS IEC 61226:2009 (Ref. 44). A cross-cutting GDA Issue has been raised to cover submission of the outcome of EDF and AREVA's classification of C&I SIS in accordance with the defined guidance and standards (see Section 4.5 for further details).

24 Smart Devices - EDF and AREVA needs to fully define the approach to be used for the justification of smart devices (i.e. devices based on computer technology) used in SIS. This type of device can be found in many types of modern equipment such as sensors, actuators, electrical protection relays and mechanical packaged plant. It is my expectation that EDF and AREVA will have arrangements that ensure such devices are identified wherever they are used in SIS and they are appropriately qualified for their

intended use. In relation to smart devices used in C&I SIS, a submission that fully defines an acceptable approach to the justification of smart devices including provision of a programme showing when implementation evidence will be available is required. I have raised a GDA Issue to cover the submission of the justification approach for smart devices and evidence of the implementation of the approach (see Section 4.3). Another concern associated with smart devices is the potential for their use, for a given Postulated Initiating Event (PIE), in multiple lines of defence. This concern is addressed by GDA Issue Action **GI-UKEPR-CI-06.A9** (see Section 4.5).

2.3.5 Out of Scope Items

25 The following items have been agreed with EDF and AREVA as being outside the scope of GDA (i.e. as identified in letter ND (NII) EPR00686N, Ref. 25).

- Turbine C&I.
- Fire protection and detection C&I.
- Waste Treatment Building C&I.
- Seismic Monitoring System.
- Fatigue, Leakage, Loose parts or Vibration Monitoring C&I.
- Radiation Monitoring C&I.
- Qualification of Excore sensors, Incore sensors and the Rod Position and Monitoring System (RPMS).
- Detailed design of the RPMS.
- Commissioning and site manuals for all C&I systems.
- NCSS detailed design, and verification and validation activities.

26 Where UK EPR information is not yet available to support the safety case, EDF and AREVA have offered equivalent FA3 information, if this has been available, as this project is at a more advanced stage than the UK EPR. For example, the PS application code was not available for GDA, however, samples of FA3 application code and lifecycle documents were provided. The FA3 documents were provided so that a better understanding of the design processes could be obtained. In Ref. 25 the following categories of scope were defined.

- Scope Category A: C&I design is defined in terms of quality plan, process, structure, function, sizing and specification for detailed design. Supporting documents associated with this category are either: specific UK EPR documents or FA3 documents with an impact analysis for changes in the C&I architecture implemented to address the issues of RI-UKEPR-002.
- Scope Category B: Definition of methodology to be adopted for specific C&I design aspects of the UK EPR. Applies to any development steps. Supporting documents associated with this category are methodology documents applicable to the UK EPR. The application of the methods was illustrated by samples from other projects, when available.
- Scope Category C: Out of GDA scope.

27 The following list, provided in Ref. 25, defines how these categories were applied to plant C&I architecture (with A / B denoting Scope Category):

- Plant I&C - Quality plan – Scope Category A;
- Plant I&C - Requirement Specification – Scope Category A;
- Plant I&C - Architecture description – Scope Category A;
- Plant I&C - Allocation of I&C functions – Scope Category A;
- Plant I&C - Test plan – Scope Category A; and
- Plant I&C - Security plan – Scope Category B.

28 Tables 1, 2, 3 and 4 below define how the principle of scope categorisation was applied. Table 1 covers the following automation systems:

- Plant Automation System (PAS);
- Safety Automation System (SAS);
- Reactor Control, Surveillance and Limitation (RCSL) System;
- Protection System (PS);
- Severe Accident (SA) I&C system;
- Non-Computerised Safety System (NCSS); and
- Priority and Actuation Control System (PACS).

29 Table 2 covers instrumentation, including the Process Instrumentation Pre-Processing System (PIPS). Table 3 covers platform development and Table 4 covers Human Machine Interface (HMI) systems, including the Process Information and Control System (PICS) and the Safety Information and Control System (SICS).

Table 1: C&I Scope Categories; Automation Systems

	PAS	SAS	RCSL	PS	SA I&C	NCSS	PACS
Quality plans	A	A	A	A	A	A	A
System specification	A	A	A	A	A	A	A
Detailed Design	B	B	B	B	B	C	C
Verification & Validation Activities	B	B	B	B	B	C	C
Commissioning & Site manuals	C	C	C	C	C	C	C

Table 2: C&I Scope Categories; Instrumentation

	Process Sensors	PIPS (sensor conditioning)	Ex-core Sensors	In-core Sensors	RPMS
Specification	A	A	A	A	A
Detailed Design	C	A	B	B	C
Qualification	B	B	C	C	C

Table 3: C&I Scope Categories; Platform Development

Set of Documentation	GDA Step 4 Scope
TELEPERM XS – Description	A
TELEPERM XS – Qualification	A
SPPA-T2000 – Description	A
SPPA-T2000 – Qualification	A
NCSS platform – Description	B
NCSS platform – Qualification	B

Table 4: C&I Scope Categories: HMI Systems

Set of documentation	GDA Step 4 scope
PICS – Specification	B
PICS – Qualification	A
SICS – Specification	B
SICS – Qualification	A

30 Insufficient information was made available during Step 4 to allow some nominally in-scope aspects of the UK EPR design to be assessed under GDA (e.g. the design of the Class 1 displays facility to be provided in the main control room). It has not been possible to include such items within this phase of assessment and appropriate GDA Issue Actions have been raised in Section 4.

3 REQUESTING PARTY'S SAFETY CASE

31 EDF and AREVA provided a number of documents setting out the UK EPR C&I safety case and also a submission outlining where the HSE SAPs are addressed in the documents. The main submission that describes the C&I is the PCSR (Ref. 22). The C&I provisions claimed include those that would be expected of a modern nuclear reactor such as:

- SSs (e.g. reactor shutdown systems such as the Protection System (PS));
- plant control and monitoring systems(e.g. the SAS, PAS and PICS);
- Main Control Room (MCR) facilities with backup via the Remote Shutdown Station (RSS); and
- communication systems for information transfer within and external to the plant.

32 EDF and AREVA's GDA Step 2 C&I submission described a conceptual design. During GDA Step 3 EDF and AREVA stated that the HSE GDA C&I assessment should be based on the FA3 design and documentation, and this concept was refined in GDA Step 4 as described in Section 2.3.6. The UK EPR makes use of two main computer-based C&I platforms, Teleperm XS (e.g. PS and RCSL system) and Siemens SPPA T2000 (e.g. PAS and SAS). At the time of the assessment the PCSR had not been updated to reflect the impact of design changes agreed under RI-UKEPR-002 (see Section 2.1 for information concerning the PCSR update).

33 An important aspect of the safety demonstration is the classification of SIS and the application of appropriate design standards. The accepted practice is that the standards are more onerous for those systems that are more important to safety (i.e. Class 1 systems are implemented using higher safety standards). In the UK, the importance to safety is typically judged by a combination of deterministic (e.g. the function performed by the system such as to shut down the reactor) and probabilistic (the reliability required of the system) criteria. The UK EPR C&I design concept reflects French custom and practice, and is largely based on French standards (e.g. RCC-E) and French regulatory requirements (see Section 4.2 for further discussion on this topic). Four function categories (i.e. F1A, F1B, F2 and NC) and equipment classes (i.e. E1A, E1B, E2 and NC) are used (see comments in Section 2.3.4).

34 The safety case assessed under GDA Step 4 consisted of the PCSR (Ref. 22), Requesting Party (RP) responses to the RI, ROs and TQs, and submissions provided by EDF and AREVA under cover of formal correspondence as listed in the Master Submission List (Ref. 23).

4 GDA STEP 4 NUCLEAR DIRECTORATE ASSESSMENT FOR C&I

35 This section documents the results of my GDA Step 4 C&I assessment and details the GDA Issues and Assessment Findings that I have raised. GDA Issues require resolution before nuclear island safety-related construction of the reactor could be considered. Assessment Findings are important to safety but are not considered critical to the decision to start nuclear island safety related construction of the reactor (see Guidance to HSE and Environment Agency Inspectors on the content of; GDA Issues, Assessment Findings, Resolution Plans, GDA Issue Metrics (Ref. 55 and see also Ref. 49)). In order to close the GDA Issues and Assessment Findings the related TSC TOs that provide further guidance will also need to be resolved. A unique TSC TO reference is used to identify the TSC's TOs (see the Annexes for the TO detail).

36 The complete GDA Issues and associated actions are formally defined in Annex 2 of this report.

4.1 Step 4 C&I SAP and Safety Case Claims-Arguments-Evidence Assessment

4.1.1 Assessment

37 This section provides the results of the assessment of the UK EPR's conformance to the HSE C&I SAPs and the adequacy of the safety case "Claims-Argument-Evidence" (CAE) trail. This Section also describes the resolution of the GDA Step 3 assessment observations.

38 A list of the HSE SAPs used to assess the adequacy of EDF and AREVA's safety case argumentation during GDA Step 3 can be found in my GDA Step 3 C&I Assessment Report (Ref. 6). In selecting the HSE SAPs for GDA Step 3 assessment, I paid particular attention to those HSE SAPs considered to have particular relevance to system and architectural design.

39 The GDA Step 3 HSE SAP argumentation assessment raised a number of observations related to adequacy of the CAE trail and HSE SAP conformance. Those addressed in this section are:

- "while EDF and AREVA claim conformance to the SAPs further argumentation and evidence will need to be provided to substantiate the claims";
- "the PCSR content does not provide adequate reference to the evidence that supports the claims".

40 The GDA Step 3 Assessment Report HSE SAP assessment observations addressed elsewhere in this report (relating to architecture, platforms and / or applications) are shown below.

- Safety Categorisation and Classification - The UK EPR 4 levels of categorisation (F1A, F1B, F2 and NC) and classification (E1A, E1B, E2 and NC) do not align with HSE SAPs (Ref. 4) or BS IEC 61226:2005 (Ref. 13) (see Sections 2.3.4 and 4.2).
- Standards - Further clarification was required in relation to the standards used by EDF and AREVA (see Section 4.2).
- Defence-in-Depth - The allocation of safety functions to C&I systems conforms to the defence-in-depth concept, aligning with the five levels referred to in the International Atomic Energy Agency (IAEA) Safety Standard NS-R-1 (Ref. 27). However, use was made of only two computer-based platforms (i.e. Teleperm XS and SPPA-T2000). It

was noted that a failure of one computer-based platform due to CCF may result in the loss of more than one level of defence (see Section 4.5).

- Redundancy - The level of equipment redundancy within the PAS and SAS required further clarification (see Section 4.4).
- Diversity - Functional and equipment diversity is used across the two computer-based platforms Teleperm XS and SPPA-T2000 but the extent required clarification (see Section 4.6).
- PS Independence - It should be demonstrated that faults in other systems will not impact on the PS safety function and that the communications are outwards from the PS (see Section 4.5).
- Reliability - The PCSR PSA gives 1 x 10^{-5} pfd and 1 x 10^{-4} pfd for the common 'Processing (non-specific)' parts of the E1A (Teleperm XS) and non-E1A (SPPA-T2000) systems respectively. These reliability claims are either beyond or at the normal limits for computer-based SS (Ref. 9) and insufficient justification of these claims was provided (see Section 4.5).
- Failure to Safety - The fail-safe principle as applied to C&I systems was not well covered in the PCSR (see Section 4.2).
- Computer-Based SIS - Further clarification was required as to how the independent confidence building and production excellence legs (for further guidance see also T/AST/046, Ref. 9) were addressed (see Section 4.2).

41 During GDA Step 4, a review of the "arguments" and "evidence" made for conformance to the HSE C&I SAPs (Ref. 4) (i.e. completion of the CAE based review against the SAPs) was completed. A list of the HSE SAPs considered during the assessment of the adequacy of EDF and AREVA's safety case argumentation during GDA Step 4 can be found in Table 5.

42 The TSC reviews performed during GDA Step 3 were based on the PCSR submitted for the start of GDA Step 3 which was dated April 2008 (Ref. 46). A revision of the PCSR was submitted in June 2009 (Ref. 47) and the TSC reviewed (see Ref. 48) the impact of the revisions to the PCSR on the conclusions to its report. The TSC determined that the June 2009 Issue 2 of the PCSR (Ref. 47) did not introduce significant improvements to the safety argumentation. A major change in PCSR Issue 2 was the introduction of references at the end of each sub-chapter. The TSC concluded that "the use of '[Ref]' at the end of a paragraph in a section within a sub-chapter is not very specific when several references are listed under this section. The system of referencing is, therefore, inefficient but does provide some link to supporting evidence. However, this may not tie in well with a particular argument against a specific SAP".

43 The ND GDA Step 3 Assessment Report determined that the safety case argumentation and identification of evidence needed improvement (Ref. 6). RO-UKEPR-62 was raised on EDF and AREVA with two actions, namely:

- to review and revise the UK EPR PCSR C&I sections so that a clear CAE trail exists within the document for all claims (Action 1);
- identify the evidence and related argument which demonstrates satisfaction of each of the HSE C&I SAPs (Action 2).

It was subsequently agreed that Action 1 could be addressed by the provision of a document referenced from the PCSR.

44 The results of the TSC's GDA Step 4 review of EDF and AREVA's HSE C&I SAP conformance demonstration and the adequacy of the safety case CAE trail is reported in the TSC GDA Step 4 report (Ref. 28). The TSC review also considered EDF and AREVA's responses to relevant Step 3 TQs and the TSC's GDA Step 3 observations, as recorded in the ND C&I Step 3 report (Ref. 6). In addition, the observations raised in the ND GDA Step 2 report have been progressed by the TSC. Those matters that remain open are recorded as TOs in the TSC's Step 4 report (Ref. 28). Annex 3 contains a summary of the TSC HSE SAP conformance and safety case CAE review, including identification of the GDA Step 4 TOs.

45 The major concern identified during GDA Step 4 relates to the closure of the CAE trail actions raised under RO-UKEPR-62. There have been a number of iterations (as a result of inadequate quality) of EDF and AREVA's submissions (i.e. in order address ND review comments). EDF and AREVA's planned final response with respect to an improved PCSR safety case CAE trail was submitted after the end of the GDA Step 4 assessment phase and has not been assessed within the timescale of this review.

46 During GDA Step 4, a part response to RO-UKEPR-62 Action 1 was assessed. While the general approach outlined by EDF and AREVA was not unacceptable, the response substantially replicates the HSE SAP CAE trail (as provided in response to Action 2) without a clear identification of the source of the claims (e.g. arising from EDF and AREVA's own safety principles, criteria and standards) and the relevant location of the claims in the PCSR (see T13.TO1.01 in Annex 3).

47 EDF and AREVA were also requested to identify the evidence and related argument that demonstrates conformance to each of the HSE C&I SAPs (RO-UKEPR-62 Action 2). The review of EDF and AREVA's responses has determined that an acceptable methodology has been developed for demonstrating conformance to the HSE SAPs. However, there are still significant shortfalls in the presented argumentation and identification of evidence for many HSE SAPs, see below.

48 The TSC performed an initial review of the adequacy of the CAE trails for all 84 HSE C&I SAPs (see Table 5). This initial review considered the adequacy of coverage of the HSE SAP requirements, argumentation and appropriateness of the identified evidence. This initial review gave rise to 44 TSC TOs (see T13.TO1.02, and T13.TO2.01 to T13.TO2.43 in Annex 3). Following this initial review, it was determined that only 68 of these SAPs were within GDA C&I scope.

49 The TSC also undertook a detailed review of the evidence identified as demonstrating conformance to a subset of the HSE C&I SAPs (i.e. 26 of the 68 C&I SAPs declared to be within the scope of GDA by EDF and AREVA). As a result of this review, 92 TOs have been raised by the various TSC tasks that undertook the detailed evidence review (see table referenced by T13.TO1.03 in Annex 3). Many of these TOs relate to minor issues, such as the inclusion of already identified references in the CAE trails. However, there are also substantive matters which need to be addressed and these are identified in the Sections below. For example, EDF and AREVA needs to ensure that the sources of its key claims (e.g. as related to its own design requirements and safety criteria) are identified.

50 By the end of the GDA Step 4 assessment, the position on the adequacy of safety case argumentation and identification of evidence (e.g. improvement of the PCSR CAE trail) was not fully satisfactory. I have raised a GDA Issue to cover the resolution of outstanding observations relating to RO-UKEPR-62 actions.

*GDA Issue: **GI-UKEPR-CI-03**; Claims, Arguments, Evidence Trail - The quality of the assessed Claims, Arguments and Evidence (CAE trail) supporting documentation provided by EDF and AREVA requires revision and improvement (RO-UKEPR-62):-*

- ***GI-UKEPR-CI-03.A1**: The CAE trail documentation provided by EDF and AREVA requires revision and improvement. EDF and AREVA to revise and improve the CAE trail documentation. In particular to:*
  - *i) review the UK EPR PCSR C&I sections and ensure that a clear CAE trail is provided for all key claims;*
  - *ii) identify the evidence and related argument which demonstrates satisfaction of each of the C&I SAPs.*

For more detailed guidance on what is required to complete this work the following TOs provide comprehensive support information: T13.TO1.01, T13.TO1.02, T13.TO1.03 (including all TOs referenced in the TO Table) and T13.TO2.01 to T13.TO2.43 in Annex 3; T16.TO2.27 in Annex 6; T17.TO2.26 in Annex 7; and T18.TO2.08 in Annex 8.

51 As a result of the assessment of:

- EDF and AREVA's demonstration of conformance to the HSE SAPs;
- the safety case CAE trail as presented in the PCSR; and
- RO-UKEPR-62 submissions,

it is concluded that, while an acceptable approach has been developed, there remain significant areas for improvement (related to GDA Issue Action **GI-UKEPR-CI-03.A1**).

4.1.2 Findings

52 The GDA Issue identified in the section above is also recorded in Annex 2.

4.2 C&I Systems' Classification and Standards

4.2.1 Assessment

53 This section reports my assessment of the company level (i.e. non-project specific) standards and guidance for C&I SIS relevant to the UK EPR. This assessment supports the assessment reported under Section 4.3 (covering the assessment of the C&I SIS platforms and pre-developed equipment proposed for the UK EPR) and Section 4.4 (covering the assessment of the C&I systems, hosted on the equipment as covered by Section 4.3). There was no equivalent assessment of company level standards and guidance reported under GDA Step 3.

54 The C&I TSC's work provided support to my assessment. The description of the scope of work performed by the TSC and the TOs arising from the work are described in a TSC report (Ref. 29). Annex 4 provides a summary of the TSC's work (Ref. 29), which includes all of the TOs.

55 The assessment of the adequacy of EDF and AREVA's company level (i.e. generic rather than project specific) C&I SIS standards was performed in a progressive, logical and thorough manner and was effectively a four step process as shown below.

1) Determination of the relevant C&I SIS standards (i.e. those defining relevant good practice) considered applicable to EDF and AREVA's company level standards. This included consideration of relevant HSE SAPs.
2) Identification of the company Quality Management System (QMS).
3) Review of the relevant RP's company level standards and identification of differences between these standards and those documents defining relevant good practice.
4) Determination of the significance of observations arising from the review, and consideration of the GDA Issues or Assessment Findings that should be raised to address any concerns.

56 I consider relevant good practice for C&I SIS to be defined in a suite of international standards produced by the International Electrotechnical Commission (IEC) based in Geneva. Standards are developed by multi-disciplined committees and are subject to international review and voting prior to issue. Issued standards are regularly reviewed and revised, as necessary, to address improvements in technologies and techniques.

57 The British technical committee NCE/8 'Reactor Instrumentation' nominates UK technical experts to the IEC committees that develop and maintain the international C&I standards. The IEC standards relevant to this assessment are identified in 'BSi Technical Committee NCE/8 Nuclear Power Plants - I&C Systems, A Guide to Applicable IEC Standards, AFP – v7 – 2008_12_01' (Ref. 37). I also considered relevant HSE SAPs (e.g. EQU.1, ECS.1, ECS.2 and ECS.3) under this aspect of my assessment.

58 The requirement for assignment of functions to categories and systems to class is set out in HSE SAPs ECS.1 and ECS.2. The relevant IEC C&I nuclear sector standard for categorisation of C&I functions is BS IEC 61226 (Ref. 44). BS IEC 61226 essentially uses deterministic criteria to place C&I functions into one of three safety Categories (i.e. A, B, or C) or identify them as non-safety / not categorised.

59 The IEC C&I nuclear sector SIS standards form a hierarchy with the top level standard BS IEC 61513 covering general requirements for SIS and overall C&I architectural requirements (Ref. 10). This standard is the nuclear sector equivalent of the generic IEC industry standard on functional safety of electrical / electronic / programmable electronic safety-related systems (see BS EN 61508 - Ref. 40), where safety-related covers all SIS.

60 Sitting below BS IEC 61513 in the hierarchy of IEC nuclear sector standards are standards addressing:

- software for CBSIS performing Category A functions (i.e. the highest safety significance), BS IEC 60880 (Ref. 17);
- software for CBSIS performing Category B and C functions, BS IEC 62138 (Ref. 36); and
- hardware design requirements for CBSIS Class 1 and 2 systems, BS IEC 60987 (Ref. 18).

EDF's QMS refers to a document produced by AFCEN (French Society for Design and Construction Rules for Nuclear Island Components) titled 'RCC-E Design and Construction Rules for Electrical components of nuclear islands' (Ref. 24). Each of the IEC standards previously mentioned in this paragraph is explicitly referenced by RCC-E, although not all relevant clauses are referenced (see T14.TO2.5 in Annex 4). Also, no guidance with respect to the use of Programmable Complex Electronic Components (PCECs) was found within RCC-E (see T14.TO1.02 in Annex 4).

61 In addition to the top-level IEC standards identified above, there are a range of supporting standards, covering topics such as equipment qualification, requirements in respect of common cause failure, segregation, and instrument and sensor specific standards (See Ref. 37).

62 Not all of the relevant requirements of the standards identified in Ref. 37 are explicitly referenced by RCC-E. However, EDF and AREVA has stated that, in addition to those standards' requirements referenced in RCC-E, other relevant standards' requirements will be referenced in project specific documents. Therefore, I have concluded that RCC-E provides necessary but not sufficient requirements and guidance for C&I SIS.

63 The use and application of relevant good practice, as defined by international standards, is an essential component of the required safety case for C&I SIS. The Licensee will need to ensure that the requirements of IEC standards not referenced by RCC-E, and as appropriate to the C&I SIS employed in the UK EPR, are addressed in the C&I SIS lifecycle. The lifecycle covers design, procurement and implementation processes, etc.

64 In response to TQ-EPR-473 (see Ref. 7), EDF and AREVA have committed to specifying all relevant IEC standards (as identified in Ref. 37) by the use of project specific documents where necessary[1]. The following Assessment Finding is raised to cover this issue for all SIS.

> *GDA Assessment Finding:* ***AF-UKEPR-CI-001*** *-The Licensee shall ensure that where RCC-E does not explicitly reference the requirements of relevant IEC SIS standards, or standard revisions (as appropriate to the C&I SIS employed in the UK EPR) these requirements are adequately addressed in the C&I SIS lifecycle covering design, procurement and implementation processes, etc. For further guidance see T14.TO1.01, T14.TO1.03, T14.TO2.01, T14.TO2.02, T14.TO2.03, T14.TO2.04, T14.TO2.05 and T14.TO2.06 in Annex 4.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]
>
> Note: GDA Issue Action GI-UKEPR-CI-06.A3 covers this issue for the PS.

65 EDF and AREVA are to provide detailed compliance matrices for a number of IEC standards (e.g. BS IEC 60880 (Ref. 17)). However, these have not been provided within the time frame of this review (see T15.TO2.06 in Annex 5). I have raised the following finding to ensure production of a comprehensive demonstration of PS (TXS), and SAS / PAS (SPPA-T2000) compliance with the key international standards.

> *GDA Assessment Finding:* ***AF-UKEPR-CI-002*** *- The Licensee shall demonstrate the compliance of the PS and associated platform with BS IEC 61513:2001, BS IEC 60880:2006 and BS IEC 60987:2007, and SAS / PAS and associated platform with BS IEC 61513:2001, BS IEC 62138:2004 and BS IEC 60987:2004. This demonstration should address platform and system requirements separately. For further guidance see T20.A1.5.2 in Annex 9; T15.TO2.05, T15.TO2.06, T15.TO2.08, T15.TO2.09, T15.TO2.10, T15.TO2.11, T15.TO1.39, T15.TO2.43 and T15.TO2.44 in Annex 5; and T16.TO1.01, T16.TO2.11, T16.TO2.28, T16.TO2.29 and T16.TO2.31 in Annex 6.*

[1] There is one exception, and that is for IEC 61504:2000 (Ref. 58), for which further justification is required, see **AF-UKEPR-CI-001,** T14.TO1.01 in Annex 4.

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

66 My GDA Step 4 assessment included a specific detailed review of a number of key Standards topics such as requirements management, independent verification and validation, and configuration management. With regard to configuration management, I found that while the standards' clauses required by RCC-E addressed configuration management at the level of individual C&I SIS, they did not address configuration management of the total C&I architecture. An overall Quality Plan (Ref. 63) was provided for assessment, and this set out the high level configuration management processes to be followed. However, the following finding is raised to ensure that configuration management arrangements are fully established for the UK EPR C&I architecture, including all SIS.

*GDA Assessment Finding: **AF-UKEPR-CI-003** - The Licensee shall demonstrate that adequate company-level processes, or UK EPR project-level processes are established for configuration management of the set of all structures, systems and components that comprise the UK EPR C&I architecture including all SIS, which should be addressed within an overall Quality Assurance Plan or equivalent, as required by BS IEC 61513:2001 clause 5.4.1. For further guidance see T14.TO1.03 in Annex 4.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

67 The application of relevant good practice to C&I SIS should be graded based upon the categorisation of safety functions as defined in BS IEC 61226:2009 (Ref. 44) and the classification of systems which perform such functions, as defined in BS IEC 61513:2001 (Ref. 10). The document referenced by EDF's QMS, RCC-E (Ref. 24), defines three Categories (i.e. F1A, F1B, F2) and Non-Categorised (NC); and three Classes (i.e. E1A, E1B, E2) and NC. These are similar but not identical to the Categories defined by Ref. 13 and the Classes defined by Ref. 10.

68 The need to adequately address categorisation and classification for the C&I aspects of the UK EPR was raised in regulatory issue RI-UKEPR-002 and was progressed under a "transverse / cross-cutting" RO (i.e. an issue covering more than one assessment discipline) on categorisation and classification, RO-UKEPR-43 (see Ref. 20).

69 A number of detailed queries were raised under RO-UKEPR-43 and submissions have been received from EDF and AREVA on this matter. The submissions included a commitment (see Ref. 42) to provide evidence to demonstrate that the classification of C&I systems is consistent with relevant good practice (e.g. to ensure that the class of the C&I systems such as the PAS and SAS align with expectations). A cross-cutting GDA Issue has been raised which contains a specific action addressing C&I categorisation and classification (i.e. cross-cutting GDA Issue Action CC-01.A6) and this is discussed further in Sections 2.3.4 and 4.5.

70 The C&I GDA Step 3 report raised two concerns (see Section 2.3.1), which have been considered further by the assessment work performed under GDA Step 4. One concern relates to the alignment of EDF and AREVA's safety categorisation and classification scheme to HSE SAPs and standards (see first bullet point below), and the other to clarification of the standards used by EDF and AREVA (see second bullet point). Both of these concerns have been addressed under GDA Step 4 as follows.

- EDF and AREVA have proposed four levels of categorisation for the UK EPR (F1A, F1B, F2 and NC) and four levels of classification (E1A, E1B, E2 and NC) and, although there are similarities, these levels do not fully align with HSE SAPs (Ref. 4) or BS IEC 61226 (Ref. 13). Cross-cutting GDA Issue Action CC-01.A6 has been raised on categorisation and classification (see above).
- EDF's QMS references RCC-E (Ref. 24) for requirements for SIS, and RCC-E references standards which are considered to constitute relevant good practice (e.g. BS IEC 60880 (Ref. 17) and BS IEC 62138 (Ref. 36)). The issue of the adequacy of EDF and AREVA's standard's coverage has already been considered in Section 4.2. EDF and AREVA have committed to provide a number of compliance matrices against relevant international standards, but these were not made available within the time frame of this review. I have raised GDA Issue Action GI-UKEPR-CI-06.A3 to cover the general issue of the demonstration of the adequacy of CBSIS, and a specific Assessment Finding (see AF-UKEPR-CI-002) to cover the compliance of the PS and SAS / PAS with key standards.

71 EDF and AREVA undertook a review of standards applicable to the security of CBSIS and has proposed an acceptable way forward in relation to implementation of a security management system for CBSIS including selection of a security assessment methodology. The following Assessment Finding is raised to address the implementation of these proposals.

*GDA Assessment Finding: **AF-UKEPR-CI-004** - The Licensee shall:*

i) demonstrate that its CBSIS security management system aligns with appropriate standards such as ISO/IEC 27001 (Ref. 43); and

ii) implement a CBSIS security assessment methodology that uses the UK government standard methodology as its foundation.

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

72 As a result of my assessment I conclude the following.

- EDF and AREVA's company-level (i.e. non-project specific) standards and guidance provide necessary but not sufficient requirements for the UK EPR C&I SIS. The company level standards will require augmentation with project-specific standards and guidance. Note that the issue of the use of appropriate standards is discussed further under Sections 4.3 and 4.4, covering UK EPR platforms and systems.
- Although a way forward with respect to categorisation and classification of UK EPR C&I SIS and equipment has been proposed, which may address my concerns in this area, further assessment of the response to the associated GDA cross-cutting Issue is required.
- An acceptable way forward has been proposed in relation to the security of CBSIS.

4.2.2 Findings

73 The Assessment Findings and GDA Issues recorded in the section above are listed in Annexes 1 and 2 respectively.

4.3 C&I SIS Platforms and Pre-Developed Equipment

4.3.1 Assessment

74 This section describes the outcome of the assessment of C&I SIS platforms and pre-developed SIS equipment for the UK EPR including the implementation of project specific standards and guidance. This assessment complements the assessment of the adequacy of company level standards and guidance reported in Section 4.2. The next section, Section 4.4, considers the implementation of standards and guidance relevant to C&I SIS (hosted on the platforms and equipment as covered by this section) of the UK EPR. Progress with resolution of the relevant GDA Step 3 observations is also specifically identified and reported.

75 My assessment was supported by the work of the C&I TSC. The description of the scope of work performed by the TSC and the TOs arising from the work are described in a TSC report (Ref. 30). Annex 5 provides a summary of the TSC's report (Ref. 30) including details of the TOs raised.

76 The topic of the compliance and alignment of EDF and AREVA's categorisation and classification methodology with relevant good practice is discussed in Section 4.2. Assessment Finding **AF-UKEPR-CI-002** was raised in Section 4.2 requiring that a demonstration of compliance of the PS and SAS/PAS, and associated platforms with relevant standards be provided. This includes the provision of a number of compliance matrices against relevant international standards which are applicable to the platforms discussed in this section (e.g. see T15.TO2.05, T15.TO2.06 and T15.TO2.09 in Annex 5 which relate to the TXS platform).

77 A risk-based approach to assessment was followed, with the greatest assessment effort allocated to those platforms and pre-developed equipment performing the most important nuclear safety functions. All assessment was performed on a sample basis.

4.3.1.1 Assessment of the Teleperm XS Platform

78 The PS platform proposed for the UK EPR is Teleperm XS (TXS) produced by AREVA. Due to the many protection functions performed by the Class 1 PS and the high reliability claims made for this system, this platform was the main focus of the GDA Step 4 assessment.

79 TXS is AREVA NP's nuclear plant C&I safety system platform. This platform was developed specifically for use in the SS of nuclear power plant. Relevant nuclear sector standards available at the time of the development of TXS were used to guide the development process (e.g. IEC 880:1986, see Ref. 17 for the current issue of this standard).

80 The scope of the platform includes the hardware components, software components and the software tools required for engineering, testing, commissioning, operation and maintenance. The qualification of the platform, including seismic qualification, was within the scope of my assessment.

81 The initial assessment of the adequacy of the TXS platform was based upon a review of documentation provided by EDF and AREVA. A number of TQs were raised as a result of this review and EDF and AREVA provided further documentation in response to those queries. In order to improve understanding between the designers and assessors, a series of technical meetings were held where issues such as the original process used to develop the platform, independent software verification, version control and the use of tools during development were reviewed. Some of these meetings were held at the

London offices of AREVA where a network link to AREVA's offices in Germany was made available. This link facilitated the review of internal company documentation on-line. These facilities were also made available for the review of the PS (see Section 4.4).

82 One of the key requirements of Ref. 17 is that SSs exhibit deterministic characteristics, and under this assessment platform characteristics such as 'predictability of execution and communication' and 'memory management' were reviewed. From the samples assessed under this review, no platform characteristics were revealed which compromised this design principle. Deterministic operation is an important factor when considering the suitability of this platform for protection system use.

83 The extent and rigour of self checking for errors, and the safe handling of any errors detected by self checking, is also a key factor I considered for this platform. A number of aspects of the design of this system concerning self checking and error handling were assessed during the GDA Step 4 review. Although no system characteristics were revealed which compromised the ability of this platform to host Class 1 systems, a number of TOs have been raised in relation to demonstrating the adequacy of self checking and error handling (i.e. T15.TO2.33, T15.TO2.34 and T15.TO2.35 in Annex 5, and T17.TO2.05 in Annex 7).

> *GDA Assessment Finding: **AF-UKEPR-CI-005** - The Licensee shall produce a comprehensive demonstration of the adequacy of Teleperm XS self checking and error handling. For further guidance see T15.TO2.33, T15.TO2.34 and T15.TO2.35 in Annex 5; and T17.TO2.05 in Annex 7.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

84 TXS is a distributed computing system which may be used in various configurations depending upon the requirements of a particular application. The TXS platform supports a four-train redundant configuration, and this is the configuration proposed for the UK EPR. The ability to support this configuration is an important factor when considering the suitability of the TXS platform for protection system use.

85 Many protection system platforms available commercially today are based on non-nuclear equipment which has been qualified for nuclear sector use some time after the original development. From the results of my assessment I have determined this is not the case for TXS, as the nuclear sector standards available at the time of the original development (some 20 years ago) were applied to guide the development process. The use of nuclear sector standards from the early stages of development is an important factor when considering the suitability of this platform for protection system use.

86 However, although EDF and AREVA have agreed to provide detailed compliance matrices for a number of IEC standards (e.g. BS IEC 60880, (Ref. 17)) these have not been provided within the time frame of this review (see T15.TO2.06 in Annex 5). I have raised GDA Issue Action **GI-UKEPR-CI-06.A3** which requires that further evidence be provided covering software production excellence. An important component of the required evidence is further demonstration of compliance against relevant international standards. An Assessment Finding has been raised under Section 4.2 to cover the issue of compliance of the TXS platform against relevant standards (see **AF-UKEPR-CI-002**).

87 The information exchanged at technical meetings and responses to TQs have greatly advanced my understanding of the TXS platform. However, responses to a number of TQs, some of which have been outstanding for many months, have not been provided within the timescale of this review (unresolved matters are also covered by TSC TOs

e.g.T15.TO2.01, T15.TO2.34, T15.TO2.35, and T15.TO2.36 in Annex 5). In particular, EDF and AREVA have not formally responded to observations arising from the TSC GDA Step 3 review (see TQ-EPR-571, Ref. 7). The TSC performed a review of these observations and identified those that were not addressed by the submissions provided during GDA Step 4, and this concern is addressed by Assessment Finding **AF-UKEPR-CI-009** (see below).

88 The initial overall C&I architecture proposed by EDF and AREVA placed reliability claims upon the Teleperm XS platform for the PS which were well beyond HSE SAP recommendations and international guidance (e.g. IAEA NS-G-1.1, Ref. 12), and this issue was raised under regulatory issue RI-UKEPR-002. In response to this issue the reliability claims were reduced to a level considered to be in alignment with standards for this type of platform. However, further justification is required in relation to substantiation of the reliability claims, and I have raised GDA Issue Action **GI-UKEPR-CI-06.A2** to address this issue (see Section 4.5).

89 An independent assessment organisation is used to support the TXS development lifecycle. However, the role of the independent assessment function does not fully align with the requirement of key nuclear sector safety standards (Refs 17 and 18) in that the independent team does not perform all assessment tasks independently, but rather reviews the scope and output of these tasks as performed by the development team.

> *GDA Assessment Finding: **AF-UKEPR-CI-006** - The Licensee shall justify all variations from the requirements of BS IEC 60880 (Ref. 17) and BS IEC 60987 (Ref. 18) with respect to the role of the independent assessor within the Teleperm XS development lifecycle, and implement compensating measures where necessary. For further guidance see T15.TO2.22 in Annex 5.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

90 The original development of the TXS was initiated in the early 1990s, and the assessment performed sampled some of the records from that time period. A number of design documents were sampled and no inconsistencies were found. However, the assessment did not identify a platform requirements specification (as required by BS IEC 61513 (Ref. 10)).

> *GDA Assessment Finding: **AF-UKEPR-CI-007** - The Licensee shall identify / produce documentation which clearly specifies the Teleperm XS platform requirements. For further guidance see T15.TO2.13 in Annex 5.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

91 My assessment reviewed samples of the platform development process. I was unable to clearly identify the process used to trace requirements through from high level to lower levels of the design, and then through to test specifications.

> *GDA Assessment Finding: **AF-UKEPR-CI-008** - The Licensee shall produce documentation which clearly identifies the traceability of requirements from the high level Teleperm XS specifications to the lower level design documents, and through to the platform test documents. For further guidance see T15.TO2.12, T15.TO2.14, T15.TO2.15 and T15.TO2.16 in Annex 5.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

92 My assessment reviewed many aspects of the TXS lifecycle and identified areas where it is considered that further justification is required in order to produce a comprehensive demonstration of the fitness for purpose of the TXS platform (e.g. failure analysis, adequacy of qualification processes, verification and type test reports).

*GDA Assessment Finding: **AF-UKEPR-CI-009** - The Licensee shall produce a comprehensive demonstration of fitness for purpose for the Teleperm XS platform which addresses, amongst others:*

- *Mean Time Between Failure analysis;*
- *adequacy of hardware lifecycle data, independent verification;*
- *adequacy of type test reports;*
- *compliance with BS IEC 60780:1998 "qualification";*
- *adequacy of Qualified Target Life;*
- *justification of the application of AREVA's 'standard approach' to qualification;*
- *adequacy of the Teleperm XS qualification process with respect to Pre-Ageing;*
- *justification that worst case timing scenarios have been used when determining processor utilisation of the Teleperm XS platform software; and*
- *justification of the adequacy of the Teleperm XS platform fault/change management process.*

For further guidance see T15.TO2.01, T15.TO2.17, T15.TO2.23, T15.TO2.24, T15.TO2.25, T15.TO2.26, T15.TO2.27, T15.TO2.28, T15.TO2.29, T15.TO2.30, T15.TO2.31, T15.TO2.32, T15.TO2.36 and T15.TO2.37 in Annex 5.

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

93 Insufficient information has been made available within the timeframe of this review to facilitate an adequate depth of review of conformance to all relevant HSE SAPs. In particular, EDF and AREVA have not provided an up to date Failure Modes and Effects Analysis (FMEA) and hardware reliability justification.

*GDA Assessment Finding: **AF-UKEPR-CI-010** - For SAP EDR.3 the evidence referenced by EDF and AREVA for PS reliability and availability is to be superseded by Failure Mode Effects Analysis calculations which were scheduled to be provided in December 2010. The Licensee shall update the CAE trail for EDR.3 and EDR.1 as appropriate, and produce the cited FMEA evidence and required justification. For further guidance see T15.TO2.50, T15.TO2.54 and T15.TO2.62 in Annex 5.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

94 For HSE SAP EDR.3 the cited evidence for CCF analysis (see also T15.TO2.57 and T15.TO2.58 in Annex 5) is qualitative with no link provided to the quantitative reliability claims that are made for the TXS platform. Therefore, I have raised GDA Issue Action

GI-UKEPR-CI-06.A2 to address the generic issue of the justification of reliability claims for SIS.

95 I have also raised GDA Issue Action **GI-UKEPR-CI-03.A1** to cover the general issue of further evidence being required to support the HSE SAP CAE trail and demonstration of conformance.

96 I had planned to perform a sample based assessment of the selection and use of Programmable Complex Electronic Components (PCECs) performing safety functions (e.g. within the TXS platform), but insufficient information was provided to facilitate such an assessment. However, my assessment did determine that there are a number of devices containing PCECs (e.g. Application Specific Integrated Circuits (ASICs) and Complex Programmable Logic Devices (CPLDs)) within the TXS platform design. The following Assessment Finding is raised to cover this issue.

> *GDA Assessment Finding: **AF-UKEPR-CI-011** - The Licensee shall produce a safety demonstration for the selection and use of Programmable Complex Electronic Components in the Teleperm XS platform, which form part of the Class 1 UK EPR Protection System, using appropriate standards and guidance. For further guidance see T14.TO1.02 in Annex 4; T15.TO1.2 and T15.TO1.3 in Annex 5; and T20.A1.5.5 in Annex 9.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

97 EDF and AREVA have proposed a programme of Independent Confidence Building Measures (ICBMs) in relation to the safety case for the TXS based PS software (see also T15.TO2.07, and T15.TO2.19 in Annex 5), but this programme has not yet been fully defined. I have raised GDA Issue Action **GI-UKEPR-CI-02.A1** to cover this issue. ND's expectations for ICBMs are outlined in a technical assessment guide (Ref. 9) and cover, for example, consideration of the application of statistical testing and static analysis of the final production software (this topic is discussed further in Section 4.5 below).

98 The United States Nuclear Regulatory Commission (US NRC) has completed a safety assessment of the TXS Platform (Ref. 38), and the assessment performed by the US NRC has been considered in my assessment (see T15.TO2.01 item 'b' in Annex 5 and Ref. 30 for further detail).

99 The UK EPR design includes a number of systems hosted on hardware platforms based on the TXS equipment family, but the highest probabilistic claims are placed on the Class 1 PS. My assessment has, therefore, focused on the use of TXS in a four-train configuration as proposed for the UK EPR PS.

100 EDF and AREVA have provided a sample of records to support claims made for this platform. Meetings were held in AREVA's London office where it was possible to:

- directly review company records relating to software requirements specification, development, testing and assessment as held on the AREVA corporate network, and
- follow documentation trails through the development and independent assessment processes.

Many of the documents reviewed at these meetings were in addition to those formally provided by EDF and AREVA to support the GDA assessment. However, there are gaps in the required evidence which I need to complete my assessment, and I have raised GDA Issues and Assessment Findings to address these gaps (as documented in this section).

101 As a result of my sample-based assessment of TXS platform I conclude that, providing the relevant GDA Issues and Assessment Findings are satisfactorily addressed, this platform is acceptable in relation to its proposed UK EPR role. Key factors guiding my judgement were:

- the deterministic behaviour of the platform;
- the reduced reliability claims now made for the PS, which is hosted on this platform;
- the option of four-train redundant configuration;
- the use of relevant nuclear sector standards to guide the development of the platform;
- the use of independent assessors during the development process; and
- the extent of self checking and error handling processes.

102 My conclusion with respect to the suitability of the TXS platform aligns with the Organisation for Economic Co-operation and Development (OECD) Multi-National Design Evaluation Programme (MDEP) common position described in Section 4.7.

4.3.1.2 Assessment of the SPPA-T2000 Platform

103 The SPPA-T2000 platform is a distributed process control and plant monitoring platform which was developed for general commercial use. It is understood that this platform has been used on conventional power stations since 1993. This platform was developed to commercial standards rather than nuclear sector standards. This platform is being installed on variants of the EPR currently under construction in France and Finland. EDF and AREVA have proposed this platform for a number of UK EPR C&I systems (e.g. the PICS, SAS and PAS). The Class 2 SAS use of this platform is the most safety significant application. Therefore, my assessment has been focused on the use of the platform in the SAS.

104 The SAS provides diverse functions (i.e. diverse to those provided by the PS) to support the provision of plant protection functions. Therefore, the SPPA-T2000 platform must be suitably qualified for use in a protection system support role. The SPPA-T2000 platform includes hardware and software components and the software tools required for engineering of the application functions, testing and commissioning, operation and maintenance. The environmental qualification of the SPPA-T2000 platform, as required for the SAS, was within the scope of assessment.

105 The platform provides the option of dual redundant processors and dual redundant input / output processors, where in the event of malfunction of an active processor, the system automatically switches to a redundant standby unit. Use of these options is proposed for the SAS and the PAS. The platform offers two communication bus options for communication between units in the same division. These options are the PAS bus (as proposed for the UK EPR PAS), and the more secure SAS bus, which consists physically of two independent busses (as proposed for the UK EPR SAS).

106 The assessment strategy took account of the lesser safety significance of this platform in the C&I architecture compared to TXS (i.e. it is used to host Class 2 and Class 3 systems, and the most demanding reliability claim made for a system hosted on this platform is $1x10^{-2}$ pfd).

107 The UK EPR safety case has a figure of $1x10^{-6}$ pfd for the total loss of C&I functions from the TXS and SPPA-T2000 platforms (Ref. 54). Considerable progress has been made in establishing the degree of diversity between these platforms. However, further detailed

analysis and evidence is required in order to demonstrate diversity of the SPPA-T2000 platform from the TXS platform and I have raised GDA Issue Action **GI-UKEPR-CI-06.A1** to address this issue.

108 The scope of my assessment included hardware design, qualification and software design. I am broadly satisfied with the results of my assessment of the records provided by EDF and AREVA to support their claims. However, insufficient information was provided by EDF and AREVA in specific technical areas (e.g. hardware development lifecycle records, compliance with platform test records, pre-developed software assessment process and the extent of environmental qualification with respect to post accident conditions) to enable me to complete a review in sufficient depth. Note that compliance against key standards is covered by **AF-UKEPR-CI-002** raised in Section 4.2.

> *GDA Assessment Finding: **AF-UKEPR-CI-012** - The Licensee shall produce a comprehensive safety demonstration addressing the adequacy of the SPPA-T2000 platform for Class 2 use covering hardware design, qualification and software design processes. For further guidance see T15.TO2.39, T15.TO2.40, T15.TO2.41, T15.TO2.42 and T15.TO2.44 in Annex 5; T17.TO2.06 in Annex 7; and T20.A2.3.4 in Annex 9.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

109 My assessment included a review of EDF and AREVA's CAE trail for a sample of applicable HSE SAPs (see Table 5). For HSE SAP ESS.15 the argument in the CAE trail provided by EDF and AREVA presents the principles for the security procedures that will be used to control access to the SPPA-T2000 Engineering System. However, no argument is presented regarding measures to ensure that the Engineering System cannot cause unintended interference with the Class 2 SAS during plant operation.

> *GDA Assessment Finding: **AF-UKEPR-CI-013** - The Licensee shall produce adequate justification that the SPPA-T2000 Engineering System cannot cause unintended interference with the Class 2 SAS during plant operation. For further guidance see T15.TO2.61 in Annex 5.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

110 I have raised GDA Issue Action **GI-UKEPR-CI-03.A1** in Section 4.1 to cover the general issue of further evidence being required to support HSE SAP conformance (for further guidance see T15.TO2.49, T15.TO2.51, T15.TO2.52, T15.TO2.53, T15.TO2.54, T15.TO2.55, T15.TO2.58, T15.TO2.59 and T15.TO2.62).

111 The SPPA-T2000 platform has been assessed, as this is the platform proposed in the current UK EPR design and this platform is being installed on EPR variants currently under construction in France and Finland. However, it is believed that elements of the SPPA-T2000 platform are obsolete and the following GDA Issue has been raised.

> *GDA Issue: **GI-UKEPR-CI-05** - Obsolescence of SPPA-T2000 platform - The EDF and AREVA C&I architecture includes systems based upon SPPA-T2000 (Siemens S5 based), but this platform is believed to be obsolete and will not be available for UK EPR:*

- ***GI-UKEPR-CI-05.A1****: The EDF and AREVA C&I architecture includes systems based upon the SPPA-T2000 (Siemens S5 based), but this platform is believed to be obsolete and will not be available for the UK EPR. EDF and AREVA needs to define the platform that will be provided for the UK EPR and submit a Basis of Safety Case (BSC) that fully addresses the change from the SPPA-T2000 (Siemens S5 based) platform to the proposed system.*

For further guidance see GI-UKEPR-CI-05.A1 in Annex 2, T15.TO1.45 in Annex 5 and T18.TO1.04 in Annex 8.

112 A Basis of Safety Case in this context is expected, amongst others, to:

- define the safety principles and standards (i.e. company, national and international) that are to be adopted for the replacement systems (i.e. incorporating the replacement platform);
- justify how these safety principles and standards will be complied with at each step of the development and deployment of the replacement systems;
- justify how functional and performance requirements will be satisfied;
- demonstrate conformance with relevant HSE SAPs;
- provide a full analysis of the impact of the replacement platform on the overall C&I design; and
- provide precise details of the change and demonstrate that the systems (covering all new components, tools and methods etc.) are fit for purpose.

113 The TSC performed a review of selected HSE SAPs relevant to the SPPA-T2000 platform. This identified a particular concern in relation to software reuse. The Licensee's adequacy of software reuse argument, as relevant to ESS.27 and ESR.5, should address all Class 2 components of the SPPA-T2000 that contain dedicated devices with embedded software, or if no such software exists, a positive statement saying so should be made. The Licensee is requested to update the CAE trail for HSE SAPs ESS.27 and ESR.5 to address this concern.

*GDA Assessment Finding: **AF-UKEPR-CI-014** - The Licensee shall ensure that the software re-use argument presented addresses all Class 2 components of the SPPA-T2000 that contain dedicated devices with embedded software, or if no such software exists a positive statement saying so should be made. For further guidance see T15.TO2.60 in Annex 5.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

114 The French regulator L'Autorité de Sûreté Nucléaire (ASN) has raised an issue concerning the adequacy of the quality system test records for the original development of the SPPA-T2000 platform, and confirmation is required that this issue does not compromise the claims made for the UK EPR design.

*GDA Assessment Finding: **AF-UKEPR-CI-015** - The Licensee shall produce adequate justification that the issue raised by ASN concerning the adequacy of the quality system test records for the original development of the SPPA-T2000 platform does not compromise the claims made for this platform in the UK EPR design. For further guidance see T15.TO1.38 in Annex 5.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

115 The generic issue of the need to adequately consider issues raised by other national regulators assessing variants of the UK EPR is considered in the following Assessment Finding.

*GDA Assessment Finding: **AF-UKEPR-CI-016** - The Licensee shall produce adequate justification that relevant issues raised by other national regulators concerning the adequacy of SIS have been adequately addressed where relevant to the UK EPR design and do not compromise the claims made for the UK EPR design.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

116 From the sample based assessment of claims, arguments and evidence I have concluded that, providing the relevant GDA Issues and Assessment Findings are satisfactorily addressed, this platform is acceptable for its proposed role. Key factors in reaching this conclusion are:

- the reduced reliability claims now made for this platform (following the changes resulting from RI-UKEPR-002);
- the addition of the NCSS to the C&I architecture; and
- the potential for dual redundant configurations of key platform components.

While broadly satisfied, the relevant GDA Issues and Assessment Findings need to be resolved.

4.3.1.3 Assessment of the NCSS Platform

117 In response to RI-UKEPR-002 EDF and AREVA have committed to modify the C&I architecture and introduce the NCSS. This system provides diversity from the computer-based PS and SAS / PAS. It has not been possible to perform an assessment of the high level design of this system as insufficient information has been made available within the timeframe of this review. I have raised GDA Issue Action **GI-UKEPR-CI-01.A1** to address this issue in Section 4.5 (see also T15.TO1.46 in Annex 5).

118 The NCSS documentation provided by EDF and AREVA to date is consistent with a diverse platform (i.e. from TXS and SPPA-T2000) being selected for the NCSS, and I consider this to be a necessary characteristic of the system platform. Sections 4.5 and 4.6 contain further detail of the NCSS concerns that I raised under RI-UKEPR-002 and a description of RP commitments made with respect to the NCSS.

4.3.1.4 Assessment of the SICS and Class 1 Display System Platform

119 I had planned to perform a sample based assessment of the Class 1 display system platform (this system is to be provided in response to concerns raised under RI-UKEPR-002). However, insufficient evidence has been made available within the timescale of this review and I have raised GDA Issue Action **GI-UKEPR-CI-06.A6** to cover this issue (see Section 4.5).

120 The SICS is based on conventional hardware and there is no ‘platform’ as such for this system. However, assessment of the SICS system is reported in Section 4.4.

4.3.1.5 Assessment of Pre-Developed Equipment

121 I had planned to perform an assessment of EDF and AREVA's arrangements covering the qualification and use of smart devices, and to perform a review of a sample of the evidence generated though the application of these arrangements. EDF and AREVA's arrangements for smart devices need to cover the processes for determining whether smart devices are used to perform nuclear safety functions, and the actual justification processes for smart devices at different safety classes. These processes have to ensure that adequate evidence is produced, which may then be made available for review. This topic has been discussed with EDF and AREVA, and a position paper provided. However, further definition of the methodology and examples of its implementation are required. A suitable submission on smart devices was not provided within the timescale of the GDA Step 4 review. I have raised the following GDA Issue to cover definition of the methodology and production of examples of the implementation of the methodology (for further guidance see also T15.TO1.48 in Annex 5), and the following Assessment Finding to address implementation of the methodology:

> *GDA Issue:* ***GI-UKEPR-CI-04*** *- Smart devices: EDF and AREVA have yet to define a methodology to be used to qualify smart devices for nuclear safety functions.*
>
> - ***GI-UKEPR-CI-04.A1****: EDF and AREVA to define the methodology to be used to qualify smart devices used in the implementation of nuclear safety functions and produce examples of the implementation of the methodology for two smart devices, one from Class 1 and one from Class 2.*
>
> *GDA Assessment Finding:* ***AF-UKEPR-CI-017*** *- The Licensee shall implement the smart devices qualification methodology defined under GDA Issue GI-UKEPR-CI-04 and ensure implementation evidence is available for review for all safety classes.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

122 The GDA scope excludes detailed design and manufacturing information for process sensors (see Section 2.3.5). However, under GDA Step 4 a review of key safety case documentation (e.g. specifications and system design manuals) for two in-core instrumentation systems was undertaken (see Annex 3). The evidence provided during GDA Step 4 did not allow the assessment against relevant IEC instrumentation standards to be completed. The Licensee will need to ensure there is an adequate safety case for such instrumentation (including demonstration of compliance to appropriate standards).

> *GDA Assessment Finding:* ***AF-UKEPR-CI-018*** *- The Licensee shall ensure there is an adequate safety case for in-core instrumentation sensors and other sensors used in SIS. For further guidance see T13.TO2.44 in Annex 3.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

4.3.2 Findings

123 The Assessment Findings and GDA Issues recorded in the section above are listed in Annex 1 and 2 respectively.

4.4 C&I Systems Important to Safety

4.4.1 Assessment

124 This section describes the outcome of the assessment of SIS, including conformance to the UK EPR project specific SIS standards and guidance. This assessment complements and builds upon the assessment reported in Sections 4.2 and 4.3. Progress with resolution of the relevant GDA Step 3 observations is specifically identified and reported.

125 The work of the C&I TSC supported my assessment. The description of the scope of work performed by the TSC, and the TOs arising from the work are described in the relevant TSC report (Ref. 31). Annex 6 provides a summary of Ref. 31 including details of the TOs raised.

126 The topic of the compliance and alignment of EDF and AREVA's categorisation and classification methodology for SIS with relevant good practice is discussed in Section 4.2, and **AF-UKEPR-CI-002** was raised to address the provision of a number of compliance matrices against relevant international standards.

127 Three ND GDA Step 3 Assessment Report (Ref. 6) observations have been considered within the scope of this part of the GDA Step 4 assessment.

1) Further information was requested concerning the level of equipment redundancy within the SAS and PAS.

EDF and AREVA provided further information in response to GDA Step 4 TQs, and through responses to Level 3 meeting actions. The technical information provided included descriptions of the:

- operation of the fault tolerant Plant bus network;
- design of the AP620 dual redundant application processor units;
- segregation of SAS into four divisions;
- operation of a communications bus within divisions to communicate between devices of the same safety class;
- SAS inter-divisional communication;
- deterministic nature of the SAS bus; and
- operation of the fault tolerant Terminal bus.

The review of the further information on equipment redundancy within the SAS and PAS provided by EDF and AREVA has not revealed any aspects of the design that are considered unacceptable. I now consider this GDA Step 3 observation to be closed.

2) It was noted that the fail-safe principle as applied to C&I systems was not well covered in the PCSR.

During GDA Step 4, EDF and AREVA clarified that the fail-safe performance for C&I nuclear safety functions (including appropriate responses to C&I equipment failure and consideration of whether or not to actuate plant items given the resultant impact on plant safety) is determined in the detailed application design stage. This approach is considered acceptable. However, the following Assessment Finding has been raised to ensure that this issue is addressed by the Licensee.

> *GDA Assessment Finding: **AF-UKEPR-CI-019** - The Licensee shall ensure the fail-safe principle (including the application of the appropriate response to C&I*

equipment failures) is implemented in the design of UK EPR C&I nuclear safety functions. For further guidance see T16.TO2.18 in Annex 6.

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

3) Further clarification was required concerning how the independent confidence building and production excellence safety case legs for CBSIS were to be addressed.

This topic is still of concern, and is covered by GDA Issue Actions **GI-UKEPR-CI-02.A1** (see later in this section) and **GI-UKEPR-CI-06.A3** (see Section 4.5).

128 EDF and AREVA defined certain aspects of the C&I design as out of scope, see Section 2.3.6, including system installation and commissioning. RCC-E (Ref. 24) requires that SIS comply with a number of international C&I standards (e.g. BS IEC 61513 (Ref. 10) and BS IEC 62138 (Ref. 36)). These standards provide requirements covering installation and commissioning but it has not been possible to review evidence covering these later system lifecycle phases for the UK EPR C&I SIS (see also T16.TO2.28 and T16.TO2.30 in Annex 6).

*GDA Assessment Finding: **AF-UKEPR-CI-020** - The Licensee shall demonstrate that the UK EPR C&I SIS comply with relevant IEC standards in their installation, commissioning and operational lifecycle phases. For further guidance see T16.TO2.28 and T16.TO2.30 in Annex 6.*

[Time: - prior to power raise.]

129 A risk-based approach to assessment was followed, with the greatest assessment effort allocated to those systems performing the most important nuclear safety functions, in particular the Class 1 PS. All assessment was performed on a sample basis (e.g. by selection of key HSE SAPs and standards' clauses for detailed review).

4.4.1.1 Assessment of the Protection System

130 The Class 1 UK EPR PS is hosted on the TXS platform configured in a four-train redundant architecture. In this configuration two-out-of-four voting on selected outputs to plant is performed. The voting logic is reduced to two-out-of-three if one train is unavailable and one-out-of-two if two trains are unavailable. I consider this configuration to be consistent with relevant good practice for protection systems, and is consistent with the configuration used on the UK's only operational PWR at Sizewell in Suffolk.

131 The production of project-specific application code and data for the TXS platform is supported by a suite of tools which were developed as part of the generic platform. These tools were within the scope of the assessment reported under Section 4.3.

132 The initial assessment of the adequacy of the PS was based upon a review of documentation provided by EDF and AREVA. In order to improve understanding between the designers and assessors, a series of technical meetings were held where aspects of the development were reviewed, such as:

- the allocation of functions to subsystems;
- the use of the platform tools to support the development of applications;
- the use of quality plans to control the applications' development process; and
- function block verification.

Some of these meetings were held at the London offices of AREVA where a network link to AREVA's offices in Germany was made available.

133 Relevant good practice for protection systems is documented in IEC standards, and I consider the most significant of these to be BS IEC 61513 (Ref. 10), BS IEC 60880 (Ref. 17) and BS IEC 60987 (Ref. 18). During the GDA Step 4 assessment, samples of development records (many based on FA3 data) were selected and reviewed. No evidence was revealed within the scope of this section's assessment which directly contradicts EDF and AREVA's claim of compliance with these standards.

134 However, it was only possible to assess EDF and AREVA's arrangements against a limited number of standards' clauses. EDF and AREVA gave a commitment to produce detailed standards' compliance matrices to improve the demonstration of standards' compliance, but these have not been provided within the time frame of this review. I have raised GDA Issue Action **GI-UKEPR-CI-06.A3** which requires EDF and AREVA to produce further evidence covering production excellence of the PS software. An important component of the required evidence is provision of the standards' compliance matrices, to further demonstrate compliance against relevant international standards (see also T16.TO1.1 in Annex 6 and Assessment Finding **AF-UKEPR-CI-002**).

135 Assessment of the application software development lifecycle revealed that, for some steps in the Verification and Validation process, the object code to be tested using the Simulation Based Validation Tool (SIVAT) tool will differ from the object code to be used on the target hardware. This is because a different compiler version will be used to generate object code for the target hardware and SIVAT. EDF and AREVA have not provided adequate justification for this aspect of the development lifecycle within the timeframe of this review.

> *GDA Assessment Finding: **AF-UKEPR-CI-021** - The Licensee shall demonstrate that the use of a different complier with the SIVAT tool compared to that used to generate the object code which will run on the PS does not compromise the integrity of the PS application software development lifecycle. For further guidance see T16.TO2.19.b in Annex 6.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

136 Assessment of the application software development lifecycle identified a concern about the adequacy of the functional test coverage of the application code which will need to be addressed.

> *GDA Assessment Finding: **AF-UKEPR-CI-022** - The Licensee shall demonstrate the adequacy of the Protection System application code testing process with respect to functional coverage. For further guidance see T16.TO2.19 item a in Annex 6.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

137 The assessment work reported under Section 4.1 covering Claims, Arguments and Evidence relevant to the HSE SAPs identified a number of SAPs relevant to the PS. It has not been possible to confirm full conformance to the following relevant sampled HSE SAPs within the timescale of this review:

- qualification records to address EQU.1 (qualification procedures), (see also T16.TO2.01 covering observations such as on the qualification of actuators and sensors);

- "design for reliability" requirements to address EDR.2 (redundancy, diversity and segregation), (see also T16.TO2.03 covering observations such as on cable separation);
- "design for reliability" requirements to address EDR.3 (common cause failure), (see also T16.TO2.04 covering this observation);
- maintenance, inspection and testing requirements to address EMT.7 (functional testing), (see also T16.TO2.05 covering observations such as on scope of testing performed);
- failure independence requirements to address ESS.18 (see also T16.TO2.06 covering observations such as on inter-module communications within the PS);
- error detection and management requirements to address ESS.21 (reliability), (see also T16.TO2.07 covering for example the handling of errors within function blocks);
- allowance for unavailability requirements to address ESS.23 (see also T16.TO2.08 in Annex 6 covering the unavailability of PS equipment); and
- scope of ICBMs to address ESS.27 (computer-based safety systems) requirements (see also T16.TO2.09 covering observations such as on the use of ICBMs), I have raised GDA Issue Action **GI-UKEPR-CI-06.A3** to cover this issue.

138 I have raised GDA Issue Action **GI-UKEPR-CI-03.A1** to cover the generic issue of the production of an adequate CAE evidence trail, and the following Assessment Finding is raised to ensure that PS conformance is demonstrated for the relevant HSE SAPs listed in the previous paragraph (the evidence trail to be addressed under GDA Issue Action **GI-UKEPR-CI-03.A1** should be updated accordingly):

> *GDA Assessment Finding: **AF-UKEPR-CI-023** - The Licensee shall demonstrate the adequacy of conformance of the Protection System with EQU.1 (qualification procedures), EDR.2 (redundancy, diversity and segregation), EDR.3 (common cause failure), EMT.7 (functional testing), ESS.18 (failure independence), ESS.21 (reliability), and ESS.23 (allowance for unavailability). For further guidance see T15.TO2.52 in Annex 5; and T16.TO2.01, T16.TO2.03, T16.TO2.04, T16.TO2.05, T16.TO2.06, T16.TO2.07 and T16.TO2.08 in Annex 6.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

139 Assessment of EDF and AREVA's response to HSE SAP ESS.7 revealed that the approach to the determination of the number of parameters provided within the PS for the initiation of safety system action did not conform to the HSE SAP requirement. The expectation is that, for those postulated initiating events where a risk reduction of $1x10^{-4}$ pfd is required from the PS there should be diversity in detection of the fault sequence. EDF and AREVA's approach is to provide two parameters for frequent postulated initiating events. To determine whether this difference in approach would challenge the HSE SAP risk targets, EDF and AREVA undertook a sensitivity study that demonstrated that for situations where there is only one PS parameter, with a claim of $1x10^{-3}$ pfd, the HSE SAP risk targets are met. See the GDA PSA Step 4 report (Ref. 41) for further details on the sensitivity study and ND's assessment thereof.

140 The PS is required to perform calculated trip functions (e.g. the departure from nucleate boiling ratio trip function), and I had intended to perform an assessment of these functions. However, insufficient information was provided by EDF and AREVA within the time scale of my assessment.

*GDA Assessment Finding: **AF-UKEPR-CI-024** - The Licensee shall produce evidence to demonstrate the adequacy of the design and implementation of the PS calculated trip functions. For further guidance see T16.TO2.33.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

141 A protection system with a full four-train redundant architecture performing a two-out-of-four voting arrangement (i.e. any two trains can initiate safety system action) should allow a train to be taken out of service. When a train is taken out of service, a two-out-of-three vote should be taken on the remaining in-service trains. The PS has a four-train architecture, but the four trains are not functionally identical. When the functions across the trains are different then the impact of taking any one of these trains out of service for maintenance will depend upon the functionality performed by that particular train. I require further clarification with respect to the impact of failures within PS trains and with respect to taking trains of the PS out of service for maintenance.

*GDA Assessment Finding: **AF-UKEPR-CI-025** - The Licensee shall demonstrate that the differences of functional coverage across the PS trains do not give rise to any safety concerns (such as an inability to meet the reliability requirements or the single failure functional criterion requirements) when failures occur within a train, or any train is taken out of service for maintenance. For further guidance see T17.TO2.09 in Annex 7, T18.TO2.01 in Annex 8 and T20.A1.4.3 in Annex 9.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

142 Of particular importance to a system such as the PS (where high reliability claims are made and computer-based technology is used with considerable design complexity) is conformance with the recommendations of HSE SAP ESS.27. In addition to production excellence, this HSE SAP requires the application of ICBMs to the final production software to provide confidence in correct operation (e.g. by performing successful statistical testing). Further guidance on ICBMs is contained in T/AST/046 (Ref. 9).

143 EDF and AREVA were not initially familiar with the concept of ICBMs and, due to lack of progress addressing the requirements of ESS.27, the issue of an adequate ICBM programme (e.g. covering statistical testing and static analysis) was raised under RI-UKEPR-002 and RO-UKEPR-58.

144 An important component of the ICBMs proposed for the PS is statistical testing. Given that the reliability claim for the PS is $1x10^{-4}$ pfd, my expectation for Statistical Testing (ST) is that 50,000 tests will be performed on the PS. This figure is based on standard statistical theory and as such is the only way that probabilistic claims can be validated for complex systems. EDF and AREVA have committed to undertake a minimum of 5,000 tests and an analysis is to be undertaken to determine the reasonable practicability of increasing the number of tests within GDA. However, it is acknowledged that, due to the need to perform this task in the later phases of the project, assessment of the results of ST and of the detailed design of the test set-up cannot be performed within the timescale of this assessment, and the following Assessment Finding is raised.

*GDA Assessment Finding: **AF-UKEPR-CI-026** - The Licensee shall implement a series of statistical-based tests (i.e. as justified in response to GDA Issue GI-UKEPR-CI-02, see below) as one component of the ICBMs for the UK EPR Protection System.*

[Time: prior to power raise.]

145 However, a more definitive view on the number of tests that it is reasonably practicable to perform on representative hardware is required. Prior to the detailed implementation to be performed during the Nuclear Site Licensing phase, I expect EDF and AREVA to more fully define the ST approach in terms of the number of tests. A commitment to perform 5,000 of these tests on representative TXS hardware has already been made and the feasibility of increasing the number of tests performed on representative hardware needs to be investigated.

146 EDF and AREVA are to investigate the potential for performing 50,000 statistical tests on a simulator as a research activity. EDF and AREVA are required to submit its analysis of the number of tests that is considered reasonably practicable to undertake on representative hardware, having given full consideration to any time and programme constraints.

147 It remains my expectation that 50,000 tests will be performed on representative TXS hardware. I consider that the plant transients should be sufficiently defined to allow a reasonably accurate definition of the time to undertake the tests to be established. I believe that undertaking this analysis and developing a monitorable programme under the scope of GDA will give good guidance to the site specific programmes sufficiently early in the process to ensure that adequate time can be given to the ST process without causing delays to the plant going into operation.

148 Other elements of the ICBM safety case leg are static analysis (SA) and compiler validation (CV). EDF and AREVA's intentions for each of these important activities needs to be fully defined. The feasibility and full extent of the application of SA to the PS application code needs to be confirmed. To date, EDF and AREVA have reported that a feasibility study indicates that the technique is viable, but EDF and AREVA have stated that further work is required to ensure the technique is scaleable and applicable to the full scope of the PS application code.

149 With regard to CV, EDF and AREVA are considering a number of options, including either the use of a Source to Code Comparison (SCC) process (similar to that used to qualify the code of the Sizewell B Primary Protection System) or the use of a compiler validation test suite. My expectation is that SCC will be performed unless a convincing argument is presented that this approach is not reasonably practicable.

150 The ICBM approach (i.e. scope, depth and rigour) needs to be fully defined before I can come to a final conclusion on the adequacy of the safety case for the PS, and the following GDA Issue is raised.

> *GDA Issue:* ***GI-UKEPR-CI-02*** *- Protection System Independent Confidence Building Measures. The programme of Independent Confidence Building Measures (ICBMs) to support the safety case for the TXS Protection System to be fully defined and agreed.*
>
> - ***GI-UKEPR-CI-02.A1:*** *The programme of Independent Confidence Building Measures (ICBMs) to support the safety case for the TXS Protection System to be fully defined and agreed. The proposed elements that will constitute the ICBMs are ST, SA and CV. For further guidance see GI-UKEPR-CI-02.A1 in Annex 2, T16.TO2.09 in Annex 6, and T15.TO2.07, T15.TO2.18 and T15.TO2.19 in Annex 5.*

151 In relation to the demonstration of the fitness for purpose of the PS, a number of requested documents were not made available within the timescale of this review. In addition, some versions of documentation provided did not align with the equipment and

processes to be used for the UK EPR PS. The following GDA Assessment Finding has been raised requiring the Licensee to address the adequacy of these items.

> *GDA Assessment Finding: **AF-UKEPR-CI-027** - The Licensee shall produce a full set of UK EPR PS development records demonstrating compliance with the requirements of the development process (e.g. D-01.3: Master Test Plan, D-01.4: Protection System - System Requirements Specification) and method documents. Traceability of requirements and qualification of tools should also be addressed. For further guidance see T16.TO2.10, T16.TO2.12, T16.TO2.13, T16.TO2.14, T16.TO2.15, T16.TO2.16, T16.TO2.17 and T16.TO2.20 in Annex 6.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

152 The findings arising from my assessment of the PS are documented in this section in GDA Issues and Assessment Findings, however, the report does not cover all the detailed assessment work performed where aspects of the PS were assessed and found to be satisfactory. A good example of such an aspect was that of inter-train PS communications. The PS design includes the use of communication links between the four redundant trains; such links have the potential to compromise the independence of trains and are a potential source of CCF across all four trains.

153 During my assessment, the justification for having such links (e.g. the four-train redundant architecture requires communications in order to perform two-out-of-four, two-out-of-three and one-out-of-two voting), and the design features which minimise the potential for such links to compromise the independence between trains and to introduce CCF were assessed. Design aspects assessed included communications protocols and arrangements for electrical segregation. The samples of data selected for assessment confirmed that the inter-train communications were constrained to the necessary exchange of information needed to perform voting of demands to initiate reactor trip or Engineered Safety Features Actuation System functions. Following my assessment, I was content that EDF and AREVA had provided adequate justification for the existence of the links and the sampled aspects of the links design that were assessed did not reveal any features that indicated the design was not adequate.

154 In conclusion, although the analysis of supporting evidence for the PS performed to date has not revealed any matters of concern which would preclude this system being used in its proposed role, there remains a significant programme of work to complete. In particular, it is essential that the current high-level proposals for ICBM activities are developed into a monitorable programme in order that I can gain sufficient confidence that adequate assessment will be performed before this system is placed in service. These concerns are reflected in the GDA Issues and Assessment Findings raised in this section of the report.

4.4.1.2 Assessment of SAS / PAS

155 The UK EPR Class 2 SAS and Class 3 PAS are to be hosted on the SPPA-T2000 platform. Although the SAS and PAS systems are hosted on the same hardware platform, the proposed configurations of these systems is different, with the design of the SAS reflecting the higher safety significance of the functions performed by this system (the SAS performs functions to back up the PS under certain fault conditions). Given the different safety significance of these systems, assessment resources have been focused on the SAS.

156 The main role of the SAS is to provide Category B and Category C safety functions. Part of the SAS is known as the Plant SAS and this part provides, amongst other functions, post-accident management automated and manual functions necessary to bring the plant to safe shutdown, functions related to support systems such as ventilation and functions preventing significant radioactivity release in the event of a severe accident occurring. There is also a part of the SAS known as the RRC-B (Risk Reduction Category – B) SAS, and this component is dedicated to severe accident RRC-B functions. The SAS is seismically qualified. In order to provide defence against common cause failures, which can be potentially generated by internal and external hazards, the SAS contains four divisions which are physically and electrically independent.

157 The main role of the PAS is the monitoring and control of the plant in all normal operating conditions. In addition, the PAS performs some monitoring and control functions related to risk reduction. The functions implemented in the PAS are categorised as F2/NC (Category C / non-categorised) by EDF and AREVA.

158 The SAS and the PAS both perform:

- data processing, data acquisition and data conditioning;
- processing of application calculations: closed loop controls, generation of individual and grouped commands (simultaneous or sequential), controls prioritisation, generation of various information intended for other I&C units etc; and
- processing of monitoring signals and the generation of alarms.

159 An assessment of the compliance of the SAS / PAS against international standards, which constitute relevant good practice, was undertaken. The relevant standards are BS IEC 61513 (Ref. 10) covering system-level requirements, BS IEC 62138 (Ref. 36) covering software requirements and BS IEC 60987 (Ref. 18) covering hardware requirements. Key supporting evidence was provided by EDF and AREVA in the form of Quality Plans, and assessment of EDF and AREVA records did not reveal any issues which indicated that the SAS / PAS systems were not appropriate for their proposed roles. Assessment against the hardware standard was limited due to insufficient records being made available by EDF and AREVA. Assessment Finding AF-UKEPR-CI-002 was raised under Section 4.2 to ensure that adequate justification for these systems against relevant good practice is provided.

160 As a result of the changes implemented in response to RI-UKEPR-002, the safety case reliability claims for the SAS have been reduced to $1x10^{-2}$ pfd. I consider that this claim is broadly compatible with my expectations for this type of system. However, although EDF and AREVA have provided a reliability justification based upon the hardware design of the platform / system, an equivalent justification for the software has not been provided, and I have raised GDA Issue Action **GI-UKEPR-CI-06.A3** to cover this issue.

161 The assessment work reported under Section 4.1 covering HSE SAPs identified a number of SAPs relevant to the SAS / PAS. It has not been possible to confirm conformance to all relevant sampled HSE SAPs within the timescale of this review, and I have raised GDA Issue Action **GI-UKEPR-CI-03.A1** to cover this issue. The TSC review has identified areas where further evidence is required in order to provide an adequate CAE trail, for example (see Annex 6):

- EDR.1 (failure to safety) - no FMEA for the SPPA-T2000 was provided (see T16.TO2.22 items a) and b));
- EDR.2 (redundancy, diversity and segregation, paragraph 170) - no consideration of systematic software failure was identified (see T16.TO2.23);

- EDR.3 (Common cause failure) - no consideration of CCF of PAS (SAS is considered) (see T16.TO2.24);
- EQU.1 (qualification procedures) - CAE trail for qualification not addressed for SPPA-T2000 (see T16.TO2.25);
- EMT.7 (functional testing) - justification of scope of periodic testing (see T16.TO2.26); and
- ESR.5 (standards for computer-based equipment) - relevant SAS information was provided but no PAS information was provided to justify standards compliance (see T16.TO2.27).

162 I have raised GDA Issue Action **GI-UKEPR-CI-03.A1** to cover the generic issue of provision of an adequate CAE evidence trail. The following Assessment Finding is raised to ensure that SAS / PAS conformance is achieved against the relevant HSE SAPs listed in the previous paragraph (the evidence trail to be addressed under GDA Issue Action **GI-UKEPR-CI-03.A1** should be updated accordingly):

> *GDA Assessment Finding: **AF-UKEPR-CI-028** - The Licensee shall demonstrate the adequacy of conformance of the SAS / PAS to EDR.1 (failure to safety), EDR.2 (redundancy, diversity and segregation), EDR.3 (Common cause failure), EQU.1 (qualification), EMT.7 (functional testing) and ESR.5 (standards for computer-based equipment). For further guidance see T16.TO2.22, T16.TO2.23, T16.TO2.24, T16.TO2.25, T16.TO2.26 and T16.TO2.27 in Annex 6.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

163 In conclusion, my assessment has not revealed any issues which would preclude the use of the SAS and PAS systems in their proposed roles. While broadly satisfied, the relevant GDA Issues and Assessment Findings need to be resolved.

4.4.1.3 Assessment of the NCSS

164 In response to RI-UKEPR-002 EDF and AREVA committed to modify the C&I architecture and introduce the Non-Computerised Safety System (NCSS). The NCSS will be implemented using diverse technology to that of the computer-based TXS and SPPA-T2000 platforms.

165 The NCSS will include the implementation of automatic functions and facilitate operator actions (after 30 minutes) as necessary to achieve a controlled state of the plant and to maintain it in a safe state for the long term. Allocation of functions to the NCSS should ensure that HSE SAP (Ref. 4) risk targets are met. The automatic functions will be implemented within the NCSS equipment in the four C&I divisions using a two-out-of-four voting logic. The manual controls will be directly hardwired to the switchgear of the actuators. Actuation will either be initiated from the main control room (from SICS) or at the switchgear level (i.e. depending on the time available under the relevant accident scenarios, as justified by human factor's analysis).

166 It has not been possible to complete the assessment of the system as insufficient information has been made available within the time frame of this review. I have raised GDA Issue Action **GI-UKEPR-CI-01.A1** (see Section 4.5) to cover this issue (see also T16.TO1.02 in Annex 6).

4.4.1.4 Assessment of Other SIS

167 The PICS is a Class 3 system that provides the main operator interface in the MCR, Technical Support Centre and the RSS. In the event of PICS failure, the SICS provides facilities to allow the operators to perform all necessary functions required with respect to maintaining plant safety. The PICS provides the display and data logging facilities I would expect of a modern Data Processing System. The PICS has a considerable level of redundancy in that formats can be displayed at any of the multiple operator workstations and communications is by dual-redundant data highway (it is noted that the plant design does not require this system to meet the single failure criteria).

168 The role of the PICS, with respect to its communications interface with the PS, has changed in response to RI-UKEPR-002 as in the original design PICS transmitted signals directly to the PS. In response to the RI, EDF and AREVA have proposed that a Class 1 Human Machine Interface (HMI) be provided, which may be used by operators to adjust and monitor PS parameters (e.g. permissives). The design of the Class 1 HMI has not been submitted within the timeframe of this assessment and I have raised GDA Issue Action **GI-UKEPR-CI-06.A6** to address this concern.

169 The Process Instrumentation Pre-Processing System (PIPS) provides signal processing (signal conditioning and / or signal multiplication) as required for the analogue and binary signals delivered by sensors and acquired by C&I systems based on the TXS platform. It also provides isolation between the sensors and downstream systems. The signals pre-processed by the PIPS are used by a number of systems, including the:

- Protection System (PS);
- Safety Automation System (SAS) for sensors shared with the PS; and
- Non-Computerised Safety System (NCSS) for the sensors shared with the PS.

170 The proposed UK EPR C&I architecture contains four sets of PIPS equipment, one located in each of the four plant divisions, with the RCC-E (Ref. 24) principles of electrical segregation to be applied between divisions.

171 TXS conditioning modules are used to implement the PIPS and these are generally designed using conventional electronics technology. However, there are some exceptions where computer-based technology is used (e.g. thermocouple signal processing modules). PIPS modules are classified depending upon their function (Class 1 to Class 3).

172 The PIPS has the potential to be the source of CCF of protection functions provided by a number of systems which are claimed to be diverse (e.g. PS, NCSS and SAS). The PIPS has a very high reliability claims and makes use of computer-based technology. Therefore, I have raised GDA Issue Action **GI-UKEPR-CI-06.A9** (see Section 4.5) to cover the production of further substantiation of the adequacy of the PIPS.

173 The Class 1 Priority and Actuation Control System (PACS) is described in the PCSR (Ref. 22) as being a system that controls and monitors each actuator under all plant operating conditions. The PACS prioritises actuation commands to the electrical switchgear powering an actuator received from the control systems (e.g. PAS) and protection systems (e.g. SAS and PS). The PACS proposed for the UK EPR will be implemented using conventional C&I technology (e.g. relays and contactors). No technical design details concerning the design proposed for the UK EPR PACS were available for assessment within the timescales of this review. I consider the correct operation of PACS to have very high nuclear safety significance.

*GDA Assessment Finding: **AF-UKEPR-CI-029** - The Licensee shall demonstrate that adequate arrangements are in place to ensure that the UK EPR Class 1 PACS meets relevant design standards, adequate defences against CCF are provided and correct prioritisation is provided. For further guidance see T17.TO2.08, T17.TO2.19 and T17.TO2.27 in Annex 7.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

174 EDF and AREVA have stated that the UK EPR SICS will be based on conventional C&I technology (e.g. push buttons, light indicators, analogue displays and recorders). Such systems are generally amenable to a rigorous safety demonstration due to their simplicity. However, insufficient information was provided to enable me to perform an assessment of the UK EPR SICS within the timeframe of this review (e.g. the SICS quality plan was included within the scope of GDA by EDF and AREVA but was not provided).

*GDA Assessment Finding: **AF-UKEPR-CI-030** - The Licensee shall demonstrate that adequate arrangements are in place to ensure that the UK EPR Class 1 SICS meets relevant design standards. For further guidance see T16.TO2.32 in Annex 6.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

175 I had planned to perform a sample based assessment of EDF and AREVA's arrangements covering the development and qualification of the Class 1 display system, which was proposed in response to RI-UKEPR-002. However, insufficient evidence was made available within the timescale of this review and GDA Issue Action **GI-UKEPR-CI-06.A6** has been raised to cover this issue (for further guidance see T16.TO1.03 in Annex 6).

176 To summarise my conclusions.

- Assessment effort has been directed at the most safety significant systems, in particular the PS. The depth and breadth of the assessment of the PS achieved reflects the priority allocated to this system.
- Assessment of the PS has not revealed any issues which would preclude its use in the UK EPR. However, there are GDA Issues and Assessment Findings that need to be resolved. Of particular importance is resolution of the scope and depth of the independent confidence building measures.
- Assessment of the SAS / PAS was limited due to the lack of documentation provided within the timescale of the review. No issues have been revealed to date which would preclude their use in the UK EPR. However, the proposed platform (SPPA-T2000 S5) may not be available for the UK EPR due to obsolescence.
- The assessment of the SICS, PIPS and PACS, was limited and GDA Issues and Assessment Findings have been raised to cover these systems.

4.4.2 Findings

177 The Assessment Findings and GDA Issues recorded in the section above are listed in Annex 1 and 2 respectively.

4.5 C&I System Level Architecture

4.5.1 Assessment

178 At the start of GDA Step 3, an initial assessment of the UK EPR C&I architecture was undertaken. In addition to my initial UK EPR architecture review, the TSC undertook a detailed review of the UK EPR C&I architecture (Ref. 52). Further review of the C&I system level architecture has been undertaken during GDA Step 4, and EDF and AREVA's responses to GDA Step 3 observations and queries raised during GDA Step 4 have been considered. An important element of the GDA Step 4 work was a review of the evidence presented by EDF and AREVA that supports the architecture related claims and arguments presented in the PCSR and identified references. A summary of the outcome of the TSC's Step 4 review of C&I system level architecture and RP responses to RI-UKEPR-002 including TOs can be found in Annexes 7 and 9 respectively.

179 The C&I system level architecture (see Ref. 22) is comprised of:

- systems implemented using the TXS platform;
  - i) Protection System,
  - ii) Reactor Control, Surveillance and Limitation System,
  - iii) Severe Accident I&C system;
- systems implemented using the SPPA-T2000 platform;
  - i) Safety Automation System,
  - ii) RRC-B Safety Automation System,
  - iii) Process Automation System,
  - iv) Process Information and Control System;
- Safety Information and Control System;
- Priority and Actuation Control System;
- Process Instrumentation Preprocessing System;
- sensors and actuators;
- networks (e.g. Class 2 network (SAS bus) and Class 3 networks (Plant bus and Terminal bus));
- Non-Computerised Safety System (introduced in response to RI-UKEPR-002); and
- Class 1 displays and controls interfacing to the Protection System (introduced in response to RI-UKEPR-002).

180 The objective of the C&I system level architecture reviews was to consider the overall system architecture (C&I systems) looking at safety design features of the UK EPR submission, namely:

- defence-in-depth and failure mode management including CCF;
- independence and diversity;
- provision for automatic and manual safety actuation; and
- appropriateness of equipment type / class.

181 It is important that the C&I architecture is based on an overall consideration of the safety functions that need to be performed, including the category and reliability of the functions.

In assigning the functions to systems, consideration needs to be given to the maintenance of independence. A key aspect of this is to establish that a failure in a lower safety class system does not frustrate the correct operation of systems of a higher safety class. Another important claim that should be justified is the robustness to failure of other systems involved in communication of important safety display information sent to the main control room. The rigorous definition of the overall system architecture, including assignment of functions to systems and definition of interface and independence requirements, assists with the demonstration that there are no safety deficiencies in the overall system architecture. Further evidence should be made available to substantiate the adequacy of the UK EPR C&I architecture.

> *GDA Assessment Finding: **AF-UKEPR-CI-031** - Definition and assignment of functions to C&I SIS - The Licensee shall ensure that for the UK EPR there is a rigorous definition of the overall system architecture, the assignment of functions to SIS, interfaces and independence requirements. For further guidance see T17.TO1.02, T17.TO1.25, T17.TO2.03, T17.TO2.10, T17.TO2.17, T17.TO2.26 and T17.TO2.27 in Annex 7; and T18.TO2.03 and T18.TO2.07 in Annex 8.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

182 The GDA Step 3 assessment revealed that the C&I architecture was overly complex with reliance on two computer-based systems (originally developed by the same company) and a high degree of connectivity between systems. My judgement was that the independence between the Class 1 PS and other SIS (Class 2 / 3) was significantly compromised.

183 A particular concern was that lower safety class systems were able to write (permissives, etc.) to higher safety class systems (i.e. the usual UK practice of only allowing one-way online communication from a safety system to systems of a lower safety class was not applied in the UK EPR design). Other significant concerns identified included:

- the absence of a safety Class 1 display system with no Class 1 manual controls or indications either in the Main Control Room or Remote Shutdown Station;
- alignment of the EPR function categories / equipment class assignments in accordance with UK expectations as defined in BS IEC 61226:2005 (Ref. 13); and
- substantiation of the reliability claims for the computer-based SIS that use the TXS and SPPA-T2000 platforms (e.g. PS, SAS and PAS).

184 I considered that the PCSR PSA reliability claims for C&I systems (i.e. 10^{-5} pfd for the common 'Processing (non-specific)' parts of the TXS PS and 10^{-4} pfd for the Siemens SPPA-T2000 platform) that provide reactor protection would prove very difficult if not impossible to substantiate. The original claim on the PS system was beyond the normal limit for reliability claims as stated in nuclear sector standards and guidance (i.e. 10^{-4} pfd), and the claim for the Siemens SPPA-T2000 platform was at the limit (for relevant guidance and standards see Refs 5, 9, 12, 13, 14 and 15, and also guidance of the French safety advisory group to ASN (Ref. 16)).

185 EDF and AREVA undertook a sensitivity study that looked at the potential for using less demanding reliability values for the computer-based C&I platforms. The sensitivity study revealed that there was unlikely to be any margin for reducing the claimed C&I system reliabilities to more credible values without significantly increasing the plant's risk estimates to levels which are close to or in excess of the HSE SAP Basic Safety Levels (i.e. Target 8 and Target 9, see Ref. 4).

186 Regulatory issue RI-UKEPR-002 was raised in relation to the concerns on the C&I architecture and this was communicated to EDF and AREVA in letter EPR70085R dated 16 April 2009 (Ref. 26). In response to RI-UKEPR-002, EDF and AREVA provided further substantiation of the UK EPR C&I design and provided a number of key commitments including to undertake a number of modifications to the UK EPR C&I architecture (Refs 50 and 54). The main commitments are summarised below:

- implementation of one way communication from the PS to the lower classified systems (exceptions to be justified on a case-by–case basis);
- classification of the SICS control and display system as Class 1, all signals transmitted between the SICS and the PS will use a Class 1 path;
- implementation of a Class 1 Qualified Display System (QDS) to provide PS commands that were previously initiated from the Class 3 PICS;
- reduction of reliability claims for the TXS (1×10^{-5} pfd to 1×10^{-4} pfd) and SPPA-T2000 (1×10^{-4} pfd to 1×10^{-2} pfd) platforms; and
- introduction of the NCSS (1×10^{-3} pfd) to provide protection and controls in case of total loss of C&I functions from the TXS and SPPA-T2000 platforms.

Note: Change modification forms (numbers 14, 15, 26 and 27) have been raised by EDF and AREVA to implement the associated design changes, see Ref. 66 for further details.

187 My assessment of EDF and AREVA's response to RI-UKEPR-002 led me to conclude that, while there were outstanding actions to complete, the majority of the key actions associated with the RI had been addressed. As a result RI-UKEPR-002 was closed in November 2010 and the remaining outstanding actions were transferred to a regulatory observation (i.e. RO-UKEPR-82). A number of RO-UKEPR-82 actions remain open and a GDA Issue has been raised to cover the necessary actions. There are nine actions under this GDA Issue on C&I Architecture and related matters.

> *GDA Issue: **GI-UKEPR-CI-06** - Issues Arising from RI-UKEPR-002 – In response to our assessment, EDF and AREVA have agreed architecture changes, categorisation changes and have committed to develop a programme of Independent Confidence Building Measures to support the EPR C&I safety case. The nine actions under this GDA issue are concerned with C&I architecture and related matters.*
>
> - ***GI-UKEPR-CI-06.A1**: EDF and AREVA to provide a comprehensive justification of diversity and independence between NCSS / PS, NCSS / SAS-PAS and PS / SAS-PAS commensurate with the level of design for a pre-construction safety report. For further guidance see **GI-UKEPR-CI-06.A1** in Annex 2; T16.TO2.21 in Annex 6; T18.TO1.03, T18.TO1.04 and T18.TO2.09 in Annex 8; and T20.A1.2.3 and T20.A1.3.4 in Annex 9.*
> - ***GI-UKEPR-CI-06.A2:** EDF and AREVA to provide a justification of the reliability figures used for each of the protection systems when claimed independently and in combination. The response should include consideration of systematic and hardware failures, and compliance with appropriate guidance and standards. For further guidance see **GI-UKEPR-CI-06.A2** in Annex 2; T16.TO2.21 in Annex 6; and T20.A1.4.1 and T20.A1.4.2 in Annex 9.*
> - ***GI-UKEPR-CI-06.A3:** EDF and AREVA to provide a justification of the approach to be used to demonstrate the adequacy of CBSIS including identification of production excellence and independent confidence building measures. For*

*further guidance see **GI-UKEPR-CI-06.A3** in Annex 2 and T20.A1.4.1.a in Annex 9. Note that the Protection System's independent confidence building measures are addressed by **GI-UKEPR-CI-02** (see Section 4.1).*

- ***GI-UKEPR-CI-06.A4:** EDF and AREVA to revise the 'Protection System – System Description NLN-F DC 193' (Ref. 56) to reflect the revised design and to provide full justification for the design, including the justification of hardwired links to the PS. For further guidance see **GI-UKEPR-CI-06.A4** in Annex 2; T17.TO1.04 in Annex 7; and T20.A2.2.1 and T20.A2.2.3 in Annex 9.*
- ***GI-UKEPR-CI-06.A5:** EDF and AREVA to provide a detailed substantiation of independence between PICS Class 3 and SAS Class 2 systems. For further guidance see **GI-UKEPR-CI-06.A5** in Annex 2 and T20.A2.3.2 in Annex 9.*
- ***GI-UKEPR-CI-06.A6:** EDF and AREVA to provide detailed substantiation of the Class 1 control and display facilities to be provided in the MCR and RSS. A BSC for the Class 1 control and display system to be provided and also a justification in terms of the functional coverage of this system. For further guidance see **GI-UKEPR-CI-06.A6** in Annex 2; T16.TO1.03 in Annex 6; T17.TO1.14, T17.TO1.15 and T17.TO2.16 in Annex 7; and T20.A3.6 in Annex 9.*
- ***GI-UKEPR-CI-06.A7:** EDF and AREVA to justify why it is not reasonably practicable for the SICS controls to be in a functional state during normal operation. For further guidance see **GI-UKEPR-CI-06.A7** in Annex 2.*
- ***GI-UKEPR-CI-06.A8:** EDF and AREVA to provide evidence, for those functions important to safety which use the Class 3 Terminal bus and / or Plant bus, that end-to-end response time requirements are achievable by design. For further guidance see **GI-UKEPR-CI-06.A8** in Annex 2; and T20.A5.4 and T20.A5.5 in Annex 9.*
- ***GI-UKEPR-CI-06.A9:** EDF and AREVA to provide detailed substantiation for the probabilistic claims for any C&I components used by more than one line of protection (e.g. sensors, smart devices, PIPS and PACS). The response to include consideration of the potential for common mode failure as a result of the use of these components. For further guidance see **GI-UKEPR-CI-06.A9** in Annex 2; T17.TO2.07, T17.TO2.08 and T17.TO2.28 in Annex 7; T18.TO1.02, T18.TO1.05 and T18.TO2.06 in Annex 8; and T20.A1.3.1 and T20.A1.3.5 in Annex 9.*

EDF and AREVA have provided submissions that might address some aspects of the above actions (e.g. **GI-UKEPR-CI-06.A4**, **GI-UKEPR-CI-06.A5** and **GI-UKEPR-CI-06.A7**) but they were provided too late for review within GDA Step 4.

188 Closure of the RI-UKEPR-002 actions on categorisation and classification were progressed under a transverse issue RO-UKEPR-43. EDF and AREVA have provided a response that addresses the concerns raised in the RI and RO (Refs 42, 50 and 57). In particular, EDF and AREVA are to ensure the classification of C&I systems is consistent with current good practice as provided by BS IEC 61226:2009 (Ref. 44).

189 The changes already committed to (e.g. SICS will be classified as Class 1, NCSS and the RCSL will be classified as Class 2, and other plant controls will be reallocated to fully comply with BS IEC 61226:2009) have substantially addressed the concern on classification raised under RI-UKEPR-002 (i.e. that a significant number of the systems were a Class lower than expectations). However, there are areas where the detailed allocation of functions to systems is not yet fully defined (e.g. implementation of diverse

lines of protection in Class 2 systems as opposed to Class 3 and reallocation of plant controls). Therefore, further detail of delivery will be required before the issue can be considered closed. GDA Issue action CC-01.A6 has been raised under cross-cutting GDA Issue **GI-UKEPR-CC-01** on Categorisation and Classification (see Ref. 65) to address this concern (e.g. to ensure the class of the C&I systems such as the Class 3 PAS and Class 2 SAS align with ND expectations).

*GDA Issue: **GI-UKEPR-CC-01** - Categorisation and Classification:*[2]

- ***GI-UKEPR-CC-01.A6**: Classification of C&I Systems. - The completion of matters arising from RI-UKEPR-002 and progressed under RO-UKEPR-43 (Action 2). Classification of C&I systems to be consistent with current good practice as provided by BS IEC 61226:2009 (Ref. 44). For further guidance see also T17.TO1.01 in Annex 7, and T20.A1.3.1.b, T20.A1.4.1.c and T20.A4.6.2 in Annex 9.*

190 EDF and AREVA have provided a commitment that the NCSS will be implemented in diverse technology to the computer-based protection systems. EDF and AREVA have defined the diversity criteria to be used in the selection of the NCSS platform (i.e. to ensure adequate diversity between the NCSS and computer-based protection systems). While EDF and AREVA have committed to provide the NCSS, the detail of the NCSS design was not made available within GDA Step 4. The GDA expectation is that adequate substantiation of the NCSS would be provided. Therefore, I have raised a GDA Issue to ensure adequate substantiation of the NCSS design.

*GDA Issue: **GI-UKEPR-CI-01** - Design Information for the Non-Computerised Safety System Required. Absence of adequate C&I architecture. The proposal to address the issues raised in RI-UKEPR-002 includes provision of a hardware based backup system known as the NCSS. Detail of the NCSS design has not been made available within GDA. EDF and AREVA have provided a commitment that the NCSS will be implemented in diverse technology to the computer based protection systems. A Basis of Safety Case for the NCSS is required for GDA.*

- ***GI-UKEPR-CI-01.A1:** EDF and AREVA to provide a Basis of Safety Case that includes substantiation of the design of the Class 2 NCSS. An action plan for completion and supply of detailed evidence supporting the basis of safety case document should also be supplied. For further guidance see GI-UKEPR-CI-01.A1 in Annex 2, and T15.TO1.46 in Annex 5, T16.TO1.02 in Annex 6, T17.TO1.24 in Annex 7 and T20.A1.2.4 in Annex 9.*

191 My assessment has determined that EDF and AREVA's defence-in-depth concept aligns with the five levels referred to in IAEA Safety Standard NS-R-1 (Ref. 27). EDF and AREVA have confirmed that the failure of a system implemented on one of the two main computer-based platforms (i.e. TXS and SPPA-T2000) is protected by functions implemented on the other platform. The introduction of the NCSS to provide protection against the total loss of the computer-based platforms has also significantly improved the C&I SIS defence-in-depth.

192 EDF and AREVA need to ensure that the PCSR is updated to take account of the changes made to address RI-UKEPR-002 and RO-UKEPR-43.

[2] A summary of this cross-cutting issue action is provided for completeness only. Please refer to Ref. 65 for a full description.

*GDA Assessment Finding: **AF-UKEPR-CI-032** - PCSR Update - The Licensee shall update the PCSR and supporting documentation to take account of the changes made to address RI-UKEPR-002 and RO-UKEPR-43. For further guidance see T17.TO1.11, T17.TO1.14 and T17.TO1.25 in Annex 7; and T18.TO1.01 in Annex 8.*

[Time: prior to fuel load.]

193 I have been encouraged by the positive response of EDF and AREVA to the concerns raised in RI-UKEPR-002 on the UK EPR C&I architecture. EDF and AREVA have proposed a way forward, which addresses the key architecture related concerns raised in RI-UKEPR-002. In particular, the commitment to provide the NCSS, introduce one way network communication from the PS to lower classified systems, Class 1 displays and manual controls, and reduction of reliability claims for the computer-based systems have addressed my major concerns. I conclude that the revised overall C&I architecture is broadly in alignment with expectations for a modern nuclear reactor, but a number of aspects related to GDA Issues and Assessment Findings require resolution, as described in this section.

4.5.2 Findings

194 The Assessment Findings and GDA Issues recorded in the section above are listed in Annex 1 and 2 respectively.

4.6 Diversity of Systems Implementing Reactor Protection Functionality

4.6.1 Assessment

195 I have completed a review of the diversity of those systems implementing reactor protection functionality. The C&I systems included in the diversity review were the PS (TXS) and SAS / PAS (Siemens SPPA-T2000). These systems were selected because they perform the UK EPR protection functions.

196 The approach included consideration of various forms of diversity, including:

- equipment diversity (including diversity of platform);
- diversity of verification and validation;
- diversity of physical location (segregation);
- software diversity;
- functional / data / signal diversity;
- diversity of design / development; and
- diversity of specification.

197 The work required the definition of a list of reactor-independent diversity characteristics derived from relevant standards and guidance. I used the HSE SAPs, TAGs, nuclear sector C&I standards (i.e. Refs 10 and 11), regulatory guidance (Ref. 5) and relevant research (Ref. 61) as a basis for determining the diversity characteristics.

198 The main finding of the preliminary review undertaken during GDA Step 3 (e.g. Ref. 53) on the diversity of systems implementing reactor protection functionality was that the submission made by EDF and AREVA for adequacy of the diversity between the primary (PS) and secondary (SAS / PAS) protection systems did not demonstrate accordance

with many of the relevant principles, standards criteria and guidance clauses used in the review. The main concerns arising from the review were:

- excessive reliability claims for the diverse protection systems;
- lack of evidence of platform diversity;
- lack of evidence of diversity within systems such as the PS when high reliability is needed; and
- absence of key information in the PCSR.

199 A major observation identified during GDA Step 3 was that the protection functions were provided by two computer-based platforms (i.e. TXS and SPPA-T2000). The introduction of the NCSS in response to RI-UKEPR-002 has addressed this concern. The adequacy of protection provided for the postulated initiating events (PIEs) by the functions implemented in the SSs has been considered in the ND fault studies assessment (Ref. 51). The fault studies assessment concluded that adequate functional diversity had not been demonstrated (e.g. across the PS and an adequately diverse protection system) and a GDA Issue (**GI-UKEPR-FS2**) has been raised to cover this topic.

200 In responding to RI-UKEPR-002, EDF and AREVA have provided further substantiation of the diversity between the TXS and SPPA-T2000 platforms, and reduced the reliability claims for these platforms. The changes proposed to the UK EPR architecture and reliability claims have been considered during the TSC's GDA Step 4 diversity review (Ref. 33). I conclude that an acceptable way forward on the major diversity concerns has been achieved. This conclusion is subject to satisfactory resolution of GDA Issue Action **GI-UKEPR-CI-06.A1** and related TOs which address, amongst other observations:

- diversity of verification and validation (covering methods, tools and programming environment, see T20.A1.3.4 in Annex 9);
- software (development tools, methods and programming environment, see T20.A1.3.4 in Annex 9); and
- communication networks such as the TXS Profibus and SPPA-T2000 'Profibus DP' (i.e. if it is used as a result of modifications to address the SPPA-T2000 obsolescence issue - see T13.TO1.04 in Annex 3).

201 The main finding to arise from the GDA Step 4 diversity assessment is that a comprehensive justification of diversity and independence between the NCSS / PS, NCSS / SAS-PAS and PS / SAS-PAS needs to be provided (see GDA Issue Action **GI-UKEPR-CI-06.A1** in Section 4.5.1). While the diversity analysis provided for the PS / SAS-PAS has indicated that they are in principle diverse, more detailed information is required before this concern can be closed. For example, a demonstration of the diversity of the TXS and SPPA-T2000 methodology for requirements specification is required (see T18.TO2.09 in Annex 8).

202 EDF and AREVA have committed to implementing the NCSS in diverse technology to that of the computer-based systems and has provided a set of diversity criteria to be used in the selection of the NCSS platform. These criteria have been reviewed and observations on areas for improvement provided to EDF and AREVA by TQ. EDF and AREVA's revision of the NCSS diversity criteria to address the areas for improvement (see T20.A1.2.3 in Annex 9) will require assessment during the GDA closure phase. This concern is covered by GDA Issue Action **GI-UKEPR-CI-06.A1** (see Section 4.5.1).

203 Substantiation of the probabilistic claims for any C&I components used by more than one SIS, and potentially by more than one line of protection (e.g. PIPS and PACS) is required.

The response on this topic needs to include consideration of the potential for common cause failure as a result of the use of these shared components. This concern is covered by GDA Issue Action **GI-UKEPR-CI-06.A9** (see Section 4.5.1). This issue relates to the use of any common components (e.g. sensors or actuators) used across more than one SIS (e.g. the same sensor type used across the PS, SAS and NCSS or PAS and PS) where a common cause failure of the components could prevent the SIS from delivering the required safety function(s) (see T18.TO1.01, T18.TO1.02 and T18.TO1.TO5 in Annex 8).

204 The GDA Step 4 assessment is based on the SPPA-T2000 S5 platform but it is believed that elements of this platform are obsolete and a new platform will be required. Therefore, the detailed diversity analysis required under GDA Issue Action **GI-UKEPR-CI-06.A1** (see Section 4.5.1) will need to take account of any changes necessary to address the SPPA-T2000 S5 obsolescence issue (see GDA Issue **GI-UKEPR-CI-05**).

205 The diversity related changes will need to be incorporated into the PCSR and supporting documentation (see Assessment Finding in 4.4.1 and TO.18.TO1.01 in Annex 8).

206 The response of EDF and AREVA to the concerns raised in RI-UKEPR-002 on the UKEPR C&I architecture have addressed my significant diversity concerns. In particular, the reduction of the reliability claims on the computer-based systems and introduction of the NCSS have addressed my major diversity concerns. I conclude that, in broad terms, the diversity of those systems implementing reactor protection functionality is acceptable but a number of aspects related to GDA Issues and Assessment Findings require resolution. For example, detailed analysis of NCSS / Teleperm TXS / SPPA-T2000 diversity and the potential for common mode failure of components used across multiple SIS / lines of protection.

4.6.2 Findings

207 No Assessment Findings or GDA Issues have been raised in this section but relevant issues and findings are raised in the previous Sections (e.g. see Section 4.5.1).

4.7 Overseas Regulatory Interface

208 ND's GDA strategy for working with overseas regulators is set out in 'Strategy for working with overseas regulators. Version 1. HSE' (Ref. 59). In accordance with this strategy, ND collaborates with overseas regulators, both bilaterally and multinationally.

4.7.1 Bilateral Collaboration

209 ND has formal information exchange arrangements to facilitate greater international co-operation with the nuclear safety regulators in a number of key countries with civil nuclear power programmes. These include:

- US NRC;
- ASN; and
- the Finnish regulator (STUK).

210 During my assessment a significant concern was identified in relation to the C&I architecture (raised with EDF and AREVA under RI-UKEPR-002). The issue was primarily around ensuring the adequacy of the SS (those used to maintain control of the plant if it goes outside normal conditions), and their independence from the control

systems (those used to operate the plant under normal conditions). Bilateral discussions were held with both ASN and STUK in relation to the C&I architecture concerns. The culmination of this collaboration was the publication of a joint regulatory position statement outlining the common view of the three regulators (Ref. 60). All parties recognised the importance of resolving the concern and undertook to progress the matter to conclusion, taking into account licensees' requirements and national regulatory requirements or practices. The way in which this issue has been resolved in the UK is discussed in Section 4.5.

4.7.2 Multilateral Collaboration

211 ND collaborates through the work of the IAEA and the OECD Nuclear Energy Agency (NEA). ND also represents the UK in MDEP - a multinational initiative taken by national safety authorities to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities tasked with the review of new reactor power plant designs. The aim of this programme is to promote consistent nuclear safety assessment standards among different countries.

212 To support the GDA C&I assessment, process insights from other regulators have been gained through participation in MDEP. ND has also shared assessment views and findings with our MDEP partners assessing EPR variants (USA, France, Finland and China) and has contributed to joint working. Some countries have more advanced plans for construction of the EPR design than the UK and it has been particularly beneficial to have had access to the experience of regulators from those countries.

213 One of the major achievements of the MDEP EPR Working Group was the development of common positions covering important C&I topics such as design complexity and independence within the C&I architecture.

214 MDEP is expected to continue beyond GDA and ND will continue to take an active role.

5 CONCLUSIONS

215 This report presents the findings of the Step 4 C&I assessment of the EDF and AREVA UK EPR reactor.

216 To conclude, I am broadly satisfied with the claims, arguments and evidence laid down within the PCSR and supporting documentation for the C&I which is included in the Submission Master List (Ref. 66). I consider that, from a C&I view point, the EDF and AREVA UK EPR design is suitable for construction in the UK. However, this conclusion is subject to satisfactory progression and resolution of GDA Issues to be addressed during the forward programme for this reactor, and the assessment of additional information that becomes available as the GDA Design Reference is supplemented with additional details on a site-by-site basis.

5.1 Key Findings from the Step 4 Assessment

217 The major conclusions of my Step 4 assessment are that:

- the PCSR and supporting documentation cover the main C&I SIS expected in a modern nuclear reactor;
- the principal design and implementation standards used by EDF and AREVA for all C&I SIS are broadly in accordance with those expected in the nuclear sector;
- EDF and AREVA's safety case for the sampled key C&I SIS and platforms used to implement the SIS is broadly in line with expectations (noting that further implementation detail needs to be added to the safety cases following design completion); and
- the significant C&I architecture concerns raised in RI-UKEPR-002 have been addressed by the introduction of a safety Class 2 Non-Computerised Safety System (NCSS), one way network communication from the Protection System (PS) to lower classified systems, Class 1 displays and manual controls, and reduction of reliability claims for the computer-based SIS.

218 Some of the observations identified within this report are of particular significance and will require resolution before ND would agree to the commencement of nuclear safety related construction of a UK EPR reactor in the UK. These are identified in this report as GDA Issues and are listed in Annex 2. In summary these relate to:

- revision of the safety case to address the introduction of the NCSS including the demonstration of its diversity from the computer-based safety systems;
- revision of the safety case to address PS changes to ensure there are only outward network communications to other systems from the PS and justification of the small number of hardwired links to the PS;
- justification of the revised reliability figures used for the protection systems (PS, SAS / PAS and NCSS) when claimed independently and in combination;
- provision of detailed substantiation of the Class 1 control and display facilities including justification of functional coverage;
- revision of the safety case to classify the C&I systems (e.g. PAS and SAS) in accordance with international standards and commitments provided by EDF and AREVA;

- finalisation of the PS independent confidence building activities' scope (covering statistical testing, static analysis and compiler validation), and definition of production excellence and independent confidence building measures for other SIS;
- enhancements to the safety case, in particular, to the presentation of the claims-arguments-evidence trail (i.e. covering key safety case claims and HSE SAP conformance);
- fully defining the approach to the justification of smart devices (based on computer technology) used in SIS including provision of a programme showing when implementation evidence will be available; and
- revision of the SAS / PAS safety case to address obsolescence of the SPPA-T2000 (Siemens S5 based) platform.

5.1.1 Assessment Findings

219 In some areas there has been a lack of detailed information, which has limited the extent of my assessment. As a result, I will need additional information to underpin my conclusion and these are identified as Assessment Findings to be carried forward as normal regulatory business, such as standards compliance demonstration for SIS and sensors, and implementation of process improvements (e.g. relating to PS requirements traceability and production of method statements). I conclude that the Assessment Findings listed in Annex 1 should be addressed during the forward programme of this reactor as part of normal regulatory business.

5.1.2 GDA Issues

220 I conclude that the GDA Issues listed in Annex 2 must be satisfactorily addressed before Consent will be granted for the commencement of nuclear island safety related construction.

6 REFERENCES

1 *GDA Step 4 Control and Instrumentation Assessment Plan for the EDF and AREVA UK EPR.* HSE-ND Assessment Plan AR 09/056. February 2010. TRIM Ref. 2009/464081.

2 ND BMS. *Assessment Process*. AST/001 Issue 4. April 2010. www.hse.gov.uk/foi/internalops/nsd/assessment/ast001.htm.

3 Not used.

4 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition Revision 1. HSE. January 2008. www.hse.gov.uk/nuclear/saps/saps2006.pdf.

5 *Licensing of Safety Critical Software for Nuclear Reactors. Common position of seven European nuclear regulators and authorised technical support organisations*. Revision 2010. www.hse.gov.uk/nuclear/software.pdf.

6 *Step 3 Control and Instrumentation Assessment of the EDF and AREVA UK EPR*. HSE-ND. AR 09/038. November 2009. TRIM Ref. 2009/339202.

7 *EDF and AREVA UK EPR - Schedule of Technical Queries Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600726.

8 *ND BMS. Safety Systems*. T/AST/003, Issue 5. September 2009. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast003.htm.

9 *ND BMS. Technical Assessment Guide - Computer Based Safety Systems*. T/AST/046 Issue 2. June 2008. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast046.htm.

10 *BS IEC 61513:2001 Nuclear power plants - Instrumentation and control for systems important to safety – general requirements for systems. International Electrotechnical Commission*. British Standard Institution (BSI) (IEC). 2001.

11 *BS IEC 62340:2007 Nuclear power plants - Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF).* International Electrotechnical Commission (IEC). 2007.

12 *Software for Computer Based Systems Important to Safety in Nuclear Power Plants*. International Atomic Energy Agency (IAEA) Safety Standards Series No. NS-G-1.1. IAEA, Vienna. 2000.

13 *BS IEC 61226:2005. Nuclear power plants. Instrumentation and Control Systems Important to Safety. Classification of instrumentation and Control Functions*. International Electrotechnical Commission (IEC). 2005.

14 *The Tolerability of Risk from Nuclear Power Stations*. HSE. 1992. ISBN 0-11-886368-1. www.hse.gov.uk/nuclear/tolerability.pdf.

15 Not used.

16 *Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Pressurized Water Plant Units* - adopted during plenary meetings of the 'Groupe Permanent Chargé des Réacteurs' and German experts on the 19 and 26 October 2000.

17 *BS IEC 60880:2006. Nuclear power plants - Instrumentation and control systems important to safety. Software aspects for computer-based systems performing category A functions*. International Electrotechnical Commission (IEC). 2006. ISBN 978 0 580 63962 3.

18 *BS IEC 60987:2007. Nuclear power plants. Instrumentation and control important to safety. Hardware design requirements for computer-based systems.* International Electrotechnical Commission (IEC). 2007. ISBN 978 0 580 63961 6.

19 Not used.

20 *EDF and AREVA UK EPR - Schedule of Regulatory Observations Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600727.

21 *EDF and AREVA UK EPR - Schedule of Regulatory Issues Raised during Step 4*. HSE-ND. TRIM Ref. 2010/600728.

22 *UK EPR Pre-Construction Safety Report – November 2009 Submission*. Submitted under cover of letter UN REG EPR00226N, 30 November 2009. TRIM Ref. 2009/481363 and as detailed in UK EPR Master Submission List. November 2009. TRIM Ref. 2011/46364.

23 *UK EPR Master Submission List*. November 2009. TRIM Ref. 2011/46364.

24 *Design and Construction Rules for Electrical Components of Nuclear Islands. RCC-E. December 2005*. ©AFCEN French Association for design, construction and in-service inspection rules for nuclear island components. ©AFCEN 105-2005.

25 *Control and Instrumentation - Scope GDA*. Letter from UK EPR Project Front Office to ND. Unique Number EPR00686N. 22 December 2010. TRIM Ref. 2010/640659.

26 *Control and Instrumentation - Architecture Regulatory Issue RI-UKEPR-002*. Letter from ND to UK EPR Project Front Office. Unique Number EPR70085R. 16 April 2009. TRIM Ref. 2009/152909.

27 Safety of Nuclear Power Plants: Design – Requirements. IAEA Safety Standards Series – No. NS-R-1. International Atomic Energy Agency (IAEA) Vienna 2000.

28 Frazer Nash/Altran Report - NII GDA Technical Review – C&I SAP Conformance and Adequacy of Safety Case Review for UKEPR Step 4 Tasks 11-13 Report. 37194/36614R. TRIM Ref. 2011/297600.

29 Frazer Nash/Altran Report - Generic Design Assessment Technical Review - C&I Step 4 Report for Task 14 - Review of EDF/Areva QMS processes against Principal Design and Implementation Standards –UK EPR. S.P1440.74.30. TRIM Ref. 2011/297636.

30 Frazer Nash/Altran Report - Generic Design Assessment Technical Review - C&I Task 15 Class 1 & 2 System Platforms and Pre-Developed Complex Components Review for UK EPR Reactor. S.P1440.74.25. TRIM Ref. 2011/297657.

31 Frazer Nash/Altran Report - Generic Design Assessment Technical Review - C&I Step 4 Report for Task 16 – Review of Systems. S.P1440.74.26. TRIM Ref. 2011/297676.

32 Frazer Nash/Altran Report - Generic Design Assessment Technical Review - C&I Step 4 Report for Task 17: Review of C&I Architecture - UK EPR. S.P1440.77.14. TRIM Ref. 2011/297709.

33 Frazer Nash/Altran Report - Generic Design Assessment Technical Review - C&I Report for Task 18: Review of Diversity of Systems contributing to Category A functions - UK EPR. S.P1440.77.15. TRIM Ref. 2011/297738.

34 Frazer Nash/Altran Report - NII GDA Technical Review - C&I - Step 4 Review of Responses to Regulatory Issue RI-UKEPR-002 - Task 20. S.P1440.80.01. TRIM Ref. 2011/297752.

35 Not used.

36 *BS EN 62138:2004. Nuclear power plants. Instrumentation and control important for safety. Software aspects for computer-based systems performing category B or C Functions.* British Standards Institution (BSI). 2004. ISBN 978 0 580 63963 0.

37 *BSI Technical Committee NCE/8 Nuclear Power Plants - I&C Systems. A Guide to Applicable IEC Standards*. AFP – v7 – 2008_12_01. TRIM ref. 2011/386499

38 *United States Nuclear Regulatory Commission Safety Evaluation Report for Siemens Power Corporation*. EMF-2110 (NP). Office of Nuclear Reactor Regulation. May 2000.

39 Not used.

40 BS EN 61508:2002. *Functional Safety of electrical/electronic/programmable electronic safety-related systems.* International Electrotechnical Commission (IEC). 2004.

41 *Step 4 Probabilistic Safety Analysis Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-019 Revision 0. TRIM Ref. 2010/581512.

42 *Control and Instrumentation – RO-UKEPR-43 – Safety Function Categorisation and SSC Classification for the UK EPR – Actions 1 and 2*. Letter from UK EPR Project Front Office to ND. Unique Number EPR00723N. 22 December 2010. TRIM Ref. 2010/640645.

43 *ISO IEC 27001:2005. Information technology - Security techniques - Information security management systems - Requirements*. International Organisation for Standardization (IOS). 2005.

44 *BS IEC 61226:2009. Nuclear power plants. Instrumentation and control important to safety. Classification of instrumentation and control functions.* British Standards Institution (BSI). 2009. ISBN 978 0 580 70133 7.

45 Not used.

46 *UK EPR Pre-construction Safety Report*. UK EPR-0002-011 Issue 00. EDF and AREVA. April 2008. Submitted under cover of EDF and AREVA Letters EPR00039R and EPR0044R (CD003, CD004, CD005 and CD006). 30 April 2008. TRIM Refs 2008/173181 and 2008/255670.

47 *UK EPR Pre-Construction Safety Report*. UK EPR-0002-132 Issue 02. EDF and AREVA. June 2009. TRIM Ref. 2011/24373.

48 NII GDA Technical Review - C&I UK EPR - PCSR Impact Assessment – 36331/3593R, Issue 1.0. June 2009. TRIM Ref. 2011/424563.

49 *New nuclear power stations. Generic Design Assessment. Guidance on the Management of GDA Outcomes*. HSE. Version 1. 23 June 2010. www.hse.gov.uk/newreactors/reports/management-gda-outcomes.pdf

50 *Control and Instrumentation – UK EPR (C&I) – Conclusions of Level 3 & 2 Meetings on 4th and 7th October 2010*. Letter from UK EPR Project Office to ND. Unique Number EPR00607N. 15 October 2010. TRIM Ref. 2010/522508.

51 *Step 4 Fault Studies – Design Basis Faults Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-020a Revision 0. TRIM Ref. 2010/581404.

52 NII GDA Technical Review – C&I System Architecture safety Review for UK EPR – S.P1440.57.11, Issue 2.2. TRIM Ref. 2011/221355.

53 NII GDA Technical Review – C&I Diversity Aspects of C&I Category A Functional systems Design Review for UK EPR – S.P1440.57.12, Issue 2.2. TRIM Ref. 2011/221404.

54 *Control and Instrumentation – RI-UKEPR-002 – C&I Architecture Issues*. Letter from UK EPR Project Office to ND. EPR00180R. 30 September 2009. TRIM Ref. 2009/386051.

55 *New Nuclear Power Stations. Generic Design Assessment. Guidance to HSE and Environment Agency Inspectors on the Content of: GDA Issues, Assessment Findings, resolution plans and GDA Issue Metrics.* HSE-ND. 3 June 2011. TRIM Ref. 2011/302633.

56 *Protection System - System Description (Pilot Study).* NLN-F DC 193 Revision B. EDF and Areva. February 2011. TRIM Ref. 2011/128840.

57 Not used.

58 *IEC 61504:2000. Nuclear power plants. Instrumentation and control systems important to safety. Plant-wide radiation monitoring.* November 2000. ISBN 0 580 36630 8.

59 *UK Generic Design Assessment: Strategy for working with overseas regulators*. HSE. March 2009. www.hse.gov.uk/newreactors/ngn04.pdf.

60 *Joint Regulatory Position Statement on the EPR Pressurised Water Reactor* (see HSE website www.hse.gov.uk/newreactors/pressurised-water-reactor.htm).

61 *Guidance on means to achieve system diversity: DIPO 6 view.* Littlewood B, Popov P, Strigini L, Version V1.0 PP_DISPO6_01, 27th October 2008.

62 *UK EPR Consolidated Pre-construction Safety Report – March 2011 Submission.* Detailed in EDF and AREVA letter UN REG EPR00997N. November 2011. TRIM Ref. 2011/552663

63 *UK EPR - Overall I&C System Quality Plan.* NLN-F DC 132 TRIM Ref. 2011/92852.

64 *BS IEC 60780:1998. Nuclear power plants — Electrical equipment of the safety system— Qualification.* British Standards Institution (BSI). 1998. ISBN 0 580 32301 3.

65 *Step 4 Cross-cutting Topics Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-032 Revision 0. TRIM Ref. 2010/581499.

66 *UK EPR Master Submission List.* UKEPR-0018-001, Issue 01, EDF and AREVA. November 2011. TRIM Ref. 2011/552512.

Table 5

Relevant Safety Assessment Principles for C&I Considered During GDA Step 4

SAP No.	Assessment Topic / SAP Title
EKP - Key Principles	
EKP.3	Defence in depth
EKP.5	Safety measures
ECS - Safety classification and standards	
ECS.1	Safety categorisation and standards
ECS.2	Safety classification of structures, systems and components
ECS.3	Standards
ECS.4	Codes and standards
ECS.5	Use of experience, tests or analysis
EQU - Equipment qualification	
EQU.1	Qualification procedures
EDR - Design for reliability	
EDR.1	Failure to safety
EDR.2	Redundancy, diversity and segregation
EDR.3	Common cause failure
EDR.4	Single failure criterion
ERL - Reliability claims	
ERL.1	Form of claims
ERL.2	Measures to achieve reliability
ERL.3	Engineered safety features
ERL.4	Margins of conservatism
ECM - Commissioning	
ECM.1	Commissioning testing
EMT - Maintenance Inspection and Testing	
EMT.1	Identification of requirements
EMT.2	Frequency
EMT.3	Type-testing
EMT.4	Validity of equipment qualification

Table 5

Relevant Safety Assessment Principles for C&I Considered During GDA Step 4

SAP No.	Assessment Topic / SAP Title
EMT.5	Procedures
EMT.6	Reliability claims
EMT.7	Functional testing
EAD - Aging and degradation	
EAD.1	Safe working life
EAD.2	Lifetime margins
EAD.3	Periodic measurement of material properties
EAD.5	Obsolescence
ELO - Layout	
ELO.1	Access
ELO.2	Unauthorised access
EHA - External and internal hazards	
EHA.10	Electromagnetic interference
ESS - Safety systems	
ESS.1	Requirement for safety systems
ESS.2	Determination of safety system requirements
ESS.3	Monitoring of plant safety
ESS.4	Adequacy of initiating variables
ESS.5	Plant interfaces
ESS.6	Adequacy of variables
ESS.7	Diversity in the detection of fault sequences
ESS.8	Automatic initiation
ESS.9	Time for human intervention
ESS.10	Definition of capability
ESS.11	Demonstration of adequacy
ESS.12	Prevention of service infringement
ESS.13	Confirmation of operating personnel
ESS.14	Prohibition of self-resetting of actions and alarms
ESS.15	Alteration of configuration, operational logic or associated data
ESS.16	No dependency on external sources of energy

Table 5

Relevant Safety Assessment Principles for C&I Considered During GDA Step 4

SAP No.	Assessment Topic / SAP Title
ESS.17	Failure identification
ESS.18	Failure independence
ESS.19	Dedication to a single task
ESS.20	Avoidance of connections to other systems
ESS.21	Reliability
ESS.22	Avoidance of spurious operation
ESS.23	Allowance for unavailability of equipment
ESS.24	Minimum operational equipment requirements
ESS.26	Maintenance and testing
ESS.27	Computer based safety systems
ESR - Control and instrumentation of safety related systems	
ESR.1	Provision in control rooms and other locations
ESR.2	Performance requirements
ESR.3	Provision of controls
ESR.4	Minimum operational equipment
ESR.5	Standards for computer based equipment
ESR.6	Power supplies
ESR.7	Communications systems
ESR.8	Monitoring of radioactive substances
ESR.9	Response of control systems to normal plant disturbances
ESR.10	Demands on safety systems in the event of control system faults
EES - Essential services	
EES.1	Provision
EES.2	Sources external to the site
EES.3	Capacity, duration, availability and reliability
EES.4	Sharing with other plants
EES.5	Cross-connections to other services
EES.6	Alternative sources
EES.7	Protection devices
EES.8	Sources external to the site

Table 5

Relevant Safety Assessment Principles for C&I Considered During GDA Step 4

SAP No.	Assessment Topic / SAP Title
EES.9	Loss of service
EHF - Human factors	
EHF.7	User interfaces
EHF.8	Personnel competence
ECV - Containment and ventilation	
ECV.6	Monitoring devices
ECV.7	Leakage monitoring
ERC - Reactor core	
ERC.2	Shutdown systems
DC - Decommissioning	
DC.1	Design and operation
DC.2	Decommissioning strategies

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Control and Instrumentation – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-001	The Licensee shall ensure that where RCC-E does not explicitly reference the requirements of relevant IEC SIS standards, or standard revisions (as appropriate to the C&I SIS employed in the UK EPR) these requirements are adequately addressed in the C&I SIS lifecycle covering design, procurement and implementation processes, etc. For further guidance see T14.TO1.01, T14.TO1.03, T14.TO2.01, T14.TO2.02, T14.TO2.03, T14.TO2.04, T14.TO2.05 and T14.TO2.06 in Annex 4.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-002	The Licensee shall demonstrate the compliance of the PS and associated platform with BS IEC 61513:2001, BS IEC 60880:2006 and BS IEC 60987:2007, and SAS / PAS and associated platform with BS IEC 61513:2001, BS IEC 62138:2004 and BS IEC 60987:2004. This demonstration should address platform and system requirements separately. For further guidance see T20.A1.5.2 in Annex 9; T15.TO2.05, T15.TO2.06, T15.TO2.08, T15.TO2.09, T15.TO2.10, T15.TO2.11, T15.TO1.39, T15.TO2.43 and T15.TO2.44 in Annex 5; and T16.TO1.01, T16.TO2.11, T16.TO2.28, T16.TO2.29 and T16.TO2.31 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-003	The Licensee shall demonstrate that adequate company-level processes, or UK EPR project-level processes are established for configuration management of the set of all structures, systems and components that comprise the UK EPR C&I architecture including all SIS, which should be addressed within an overall Quality Assurance Plan or equivalent, as required by BS IEC 61513:2001 clause 5.4.1. For further guidance see T14.TO1.03 in Annex 4.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Control and Instrumentation – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-004	The Licensee shall: i) demonstrate that its CBSIS security management system aligns with appropriate standards such as ISO/IEC 27001 (Ref. 43); and ii) implement a CBSIS security assessment methodology that uses the UK government standard methodology as its foundation.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-005	The Licensee shall produce a comprehensive demonstration of the adequacy of Teleperm XS self checking and error handling. For further guidance see T15.TO2.33, T15.TO2.34 and T15.TO2.35 in Annex 5; and T17.TO2.05 in Annex 7.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-006	The Licensee shall justify all variations from the requirements of BS IEC 60880 (Ref.17) and BS IEC 60987 (Ref.18) with respect to the role of the independent assessor within the Teleperm XS development lifecycle, and implement compensating measures where necessary. For further guidance see T15.TO2.22 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-007	The Licensee shall identify / produce documentation which clearly specifies the Teleperm XS platform requirements. For further guidance see T15.TO2.13 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-008	The Licensee shall produce documentation which clearly identifies the traceability of requirements from the high level Teleperm XS specifications to the lower level design documents, and through to the platform test documents. For further guidance see T15.TO2.12, T15.TO2.14 and T15.TO2.15 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Control and Instrumentation – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-009	The Licensee shall produce a comprehensive demonstration of fitness for purpose for the Teleperm XS platform which addresses, amongst others: • Mean Time Between Failure analysis; • adequacy of hardware lifecycle data, independent verification; • adequacy of type test reports; • compliance with BS IEC 60780:1998 "qualification"; • adequacy of Qualified Target Life; • justification of the application of AREVA's 'standard approach' to qualification; • adequacy of the TXS qualification process with respect to Pre-Ageing ; • justification that worst case timing scenarios have been used when determining processor utilisation of the TELEPERM XS platform software; and • justification of the adequacy of the TXS platform fault/change management process. For further guidance see T15.TO2.01, T15.TO2.17, T15.TO2.23, T15.TO2.24, T15.TO2.25, T15.TO2.26, T15.TO2.27, T15.TO2.28, T15.TO2.29, T15.TO2.30, T15.TO2.31, T15.TO2.32, T15.TO2.36 and T15.TO2.37 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-010	For SAP EDR.3 the evidence referenced by EDF and AREVA for PS reliability and availability is to be superseded by Failure Mode Effects Analysis calculations which were scheduled to be provided in December 2010. The Licensee shall update the CAE trail for EDR.3 and EDR.1 as appropriate, and produce the cited FMEA evidence and required justification. For further guidance see T15.TO2.50, T15.TO2.54 and T15.TO2.62 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Control and Instrumentation – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-011	The Licensee shall produce a safety demonstration for the selection and use of Programmable Complex Electronic Components in the Teleperm XS platform, which form part of the Class 1 UK EPR Protection System, using appropriate standards and guidance. For further guidance see T14.TO1.02 in Annex 4; T15.TO1.2 and T15.TO1.3 in Annex 5; and T20.A1.5.5 in Annex 9.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-012	The Licensee shall produce a comprehensive safety demonstration addressing the adequacy of the SPPA-T2000 platform for Class 2 use covering hardware design, qualification and software design processes. For further guidance see T15.TO2.39, T15.TO2.40, T15.TO2.41, T15.TO2.42 and T15.TO2.44 in Annex 5; T17.TO2.06 in Annex 7; and T20.A2.3.4 in Annex 9.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-013	The Licensee shall produce adequate justification that the SPPA-T2000 Engineering System cannot cause unintended interference with the Class 2 SAS during plant operation. For further guidance see T15.TO2.61 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-014	The Licensee shall ensure that the software re-use argument presented addresses all Class 2 components of the SPPA-T2000 that contain dedicated devices with embedded software, or if no such software exists a positive statement saying so should be made. For further guidance see T15.TO2.60 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-015	The Licensee shall produce adequate justification that the issue raised by ASN concerning the adequacy of the quality system test records for the original development of the SPPA-T2000 platform does not compromise the claims made for this platform in the UK EPR design. For further guidance see T15.TO1.38 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Control and Instrumentation – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-016	The Licensee shall produce adequate justification that relevant issues raised by other national regulators concerning the adequacy of SIS have been adequately addressed where relevant to the UK EPR design and do not compromise the claims made for the UK EPR design.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-017	The Licensee shall implement the smart devices qualification methodology defined under GDA Issue GI-UKEPR-CI-04 and ensure implementation evidence is available for review for all safety classes.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-018	The Licensee shall ensure there is an adequate safety case for in-core instrumentation sensors and other sensors used in SIS. For further guidance see T13.TO2.44 in Annex 3.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-019	The Licensee shall ensure the fail-safe principle (including the application of the appropriate response to C&I equipment failures) is implemented in the design of UK EPR C&I nuclear safety functions. For further guidance see T16.TO2.18 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-020	The Licensee shall demonstrate that EPR C&I SIS comply with relevant IEC standards in their installation, commissioning and operational lifecycle phases. For further guidance see T16.TO2.28 and T16.TO2.30 in Annex 6.	Prior to power raise.
AF-UKEPR-CI-021	The Licensee shall demonstrate that the use of a different complier with the SIVAT tool compared to that used to generate the object code which will run on the PS does not compromise the integrity of the PS application software development lifecycle. For further guidance see T16.TO2.19.b in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-022	The Licensee shall demonstrate the adequacy of the Protection System application code testing process with respect to functional coverage. For further guidance see T16.TO2.19 item a) in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Control and Instrumentation – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-023	The Licensee shall demonstrate the adequacy of conformance of the Protection System with EQU.1 (qualification procedures), EDR.2 (redundancy, diversity and segregation), EDR.3 (common cause failure), EMT.7 (functional testing), ESS.18 (failure independence), ESS.21 (reliability), and ESS.23 (allowance for unavailability). For further guidance see T15.TO2.52 in Annex 5; T16.TO2.01, T16.TO2.03, T16.TO2.04, T16.TO2.05, T16.TO2.06, T16.TO2.07 and T16.TO2.08 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-024	The Licensee shall produce evidence to demonstrate the adequacy of the design and implementation of the PS calculated trip functions. For further guidance see T16.TO2.33.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-025	The Licensee shall demonstrate that the differences of functional coverage across the PS trains do not give rise to any safety concerns (such as an inability to meet the reliability requirements or the single failure functional criterion requirements) when failures occur within a train, or any train is taken out of service for maintenance. For further guidance see T17.TO2.09 in Annex 7, T18.TO2.01 in Annex 8 and T20.A1.4.3 in Annex 9.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-026	The Licensee shall implement a series of statistical-based tests (i.e. as justified in response to GDA Issue GI-UKEPR-CI-02, see below) as one component of the ICBMs for the UK EPR Protection System.	Prior to power raise.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Control and Instrumentation – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-027	The Licensee shall produce a full set of UK EPR PS development records demonstrating compliance with the requirements of the development process (e.g. D-01.3: Master Test Plan, D-01.4: Protection System - System Requirements Specification) and method documents. Traceability of requirements and qualification of tools should also be addressed. For further guidance see T16.TO2.10, T16.TO2.12, T16.TO2.13, T16.TO2.14, T16.TO2.15, T16.TO2.16, T16.TO2.17 and T16.TO2.20 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-028	The Licensee shall demonstrate the adequacy of conformance of the SAS / PAS to EDR.1 (failure to safety), EDR.2 (redundancy, diversity and segregation), EDR.3 (Common cause failure), EQU.1 (qualification), EMT.7 (functional testing) and ESR.5 (standards for computer-based equipment). For further guidance see T16.TO2.22, T16.TO2.23, T16.TO2.24, T16.TO2.25, T16.TO2.26 and T16.TO2.27 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-029	The Licensee shall demonstrate that adequate arrangements are in place to ensure that the UK EPR Class 1 PACS meets relevant design standards, adequate defences against CCF are provided and correct prioritisation is provided. For further guidance see T17.TO2.08, T17.TO2.19 and T17.TO2.27 in Annex 7.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-030	The Licensee shall demonstrate that adequate arrangements are in place to ensure that the UK EPR Class 1 SICS meets relevant design standards. For further guidance see T16.TO2.32 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.

Annex 1

Assessment Findings to Be Addressed During the Forward Programme as Normal Regulatory Business

Control and Instrumentation – UK EPR

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-CI-031	Definition and assignment of functions to C&I SIS - The Licensee shall ensure that for the UK EPR there is a rigorous definition of the overall system architecture, the assignment of functions to SIS, interfaces and independence requirements. For further guidance see T17.TO1.02, T17.TO1.25, T17.TO2.03, T17.TO2.10, T17.TO2.17, T17.TO2.26 and T17.TO2.27 in Annex 7; and T18.TO2.03 and T18.TO2.07 in Annex 8.	Prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.
AF-UKEPR-CI-032	PCSR Update - The Licensee shall update the PCSR and supporting documentation to take account of the changes made to address RI-UKEPR-002 and RO-UKEPR-43. For further guidance see T17.TO1.11, T17.TO1.14 and T17.TO1.25 in Annex 7; and T18.TO1.01 in Annex 8.	Prior to fuel load.

Note: It is the responsibility of the Licensees / Operators to have adequate arrangements to address the Assessment Findings. Future Licensees / Operators can adopt alternative means to those indicated in the findings which give an equivalent level of safety.

For Assessment Findings relevant to the operational phase of the reactor, the Licensees / Operators must adequately address the findings during the operational phase. For other Assessment Findings, it is the regulators' expectation that the findings are adequately addressed no later than the milestones indicated above.

Annex 2

GDA Issues – Control and Instrumentation – UK EPR

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
DESIGN INFORMATION FOR NON-COMPUTERISED SAFETY SYSTEM REQUIRED
GI-UKEPR-CI-01 REVISION 2

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-01**	**GDA Issue Action Reference**	**GI-UKEPR-CI-01.A1**
GDA Issue	Absence of adequate C&I architecture. The proposal to address the issues raised in RI 02 includes provision of a hardware based backup system known as the NCSS. Detail of the NCSS design has not been made available within GDA. EDF and AREVA have provided a commitment that the NCSS will be implemented in diverse technology to the computer based protection systems. A Basis of Safety Case for the NCSS is required for GDA.		
GDA Issue Action	EDF and AREVA to provide a Basis of Safety Case (BSC) that includes substantiation of the design of the Class 2 Non-Computerised Safety System. An action plan for completion and supply of detailed evidence supporting the basis of safety case document should also be supplied. The BSC should consider: • The safety principles and standards (i.e. company, national and international) that EDF and AREVA has adopted for the NCSS. • The identification of arguments for assigning safety functions and performance requirements to the NCSS in compliance with these principles and standards. • The basis of the safety case should demonstrate how the safety principles and standards adopted have or will be complied with at each step of the development and deployment of the NCSS. • It should outline why the NCSS is considered to be fit for purpose and demonstrate how all of the safety principle, standards, functional and performance requirements will be satisfied. • It is expected that these demonstrations and examinations would identify the detailed evidence supporting the claims and arguments. • The BSC is also expected to identify any supporting analysis such as hazards analysis, FMEAs, reliability analysis, environmental qualification and link them to claims made and the demonstration of fitness for purpose of the systems. • It is expected that in undertaking this exercise compliance with ONR's SAPS would also be demonstrated with deviations justified. • The BSC should describe the system, breaking it down such that the major elements can be identified (such as input/output and logic cards). The BSC should include the demonstration of adequacy for each of these elements (including identification of revisions) as well as the NCSS as a whole. • The BSC should set down the production excellence arguments and identify the independent confidence building measures. • The BSC should describe the project QA arrangements, e.g. ISO 9001, this		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

DESIGN INFORMATION FOR NON-COMPUTERISED SAFETY SYSTEM REQUIRED

GI-UKEPR-CI-01 REVISION 2

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-01**	**GDA Issue Action Reference**	**GI-UKEPR-CI-01.A1**

should include a clear description of the interface to the NCSS supplier (and any other suppliers). The BSC would also be expected to outline the NCSS supplier QA arrangements.

- The BSC should identify the pedigree of any COTS, pre-developed components as this might influence how they are justified for use.
- The BSC should demonstrate that the management arrangements for COTS/pre-developed components has been and remains adequate. This demonstration should cover, amongst others, configuration management, collection of Operating Experience and any changes along with their cause and how the change was implemented (capturing the evolution of the QA regime and processes by which this has been done).
- The BSC should address the process by which the individual components will be brought together and integrated as a system. It is anticipated this would be detailed in the BSC (or other documents referenced from the BSC) covering factory and commissioning testing as well as environmental qualification work that might be called upon to support system justification. For completeness, it should also address through life operating and maintenance, for example identifying the scope and frequency of any proof testing that is required.
- Should elements of the implementation of the NCSS system make use of complex electronic devices e.g. FPGAs (but not microprocessors) then the basis of the safety case would be expected to demonstrate how the design and implementation of the NCSS complies with relevant EDF/Areva safety principles and standards. The basis of safety case should also identify how ND guidance, for example, that contained in ESS.21 which requires the safety demonstration to include measures such as independent third party assessment (para. 355) will be addressed. Given the programmable nature of such complex devices, the justification should draw on elements of ESS.27 and the special case procedure with an argument of excellence in production and independent confidence building in respect of the systems fitness for purpose. It is expected, as above, that the demonstration would identify the detailed evidence supporting the claims and arguments made.

For further guidance see also T15.TO1.46 in Annex 5, T16.TO1.02 in Annex 6, T17.TO1.24 in Annex 7 and T20.A1.2.4 in Annex 9.

With agreement from the Regulator this action may be completed by alternative means.

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
PROTECTION SYSTEM INDEPENDENT CONFIDENCE BUILDING MEASURES
GI-UKEPR-CI-02 REVISION 2

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-02**	**GDA Issue Action Reference**	**GI-UKEPR-CI-02.A1**
GDA Issue	The programme of Independent Confidence Building Measures (ICBMs) to support the safety case for the TXS Protection System to be fully defined and agreed.		
GDA Issue Action	The programme of Independent Confidence Building Measures to support the safety case for the TXS Protection System to be fully defined and agreed. The proposed elements that will constitute the ICBMs are: • Statistical testing (ST) EDF and AREVA have proposed 5000 tests on the TXS equipment with the potential for 50000 on a simulator to be investigated as a research activity. ONR expects the RP to more fully define the ST approach in terms of number of tests. The RP is required to submit its analysis of the number of tests that it considers is reasonably practicable to undertake having given full consideration to any time and programme constraints. It remains ONR's expectation that 50,000 tests will be performed. ONR considers that the plant transients are sufficiently defined to allow a reasonably accurate definition of the time to undertake the tests to be established. Undertaking this analysis will give good guidance to the site specific programmes sufficiently early in the process to ensure that adequate time can be given to the statistical testing process without causing delays to the plant going into operation. In addition the RP needs to demonstrate, by the provision of a monitorable programme, that all of the activities required to implement ST have been defined and can be delivered to a timescale which allows ST to commence following completion of Factory Acceptance Testing of the PS (i.e. the final validation activity before the equipment is shipped to site). It should be noted the ICBM activities should be undertaken on the final version of the software (i.e. following the end of the software production process – see ONR TAG 46). The activities required to undertake ST are defined in a report produced by CINIF (Ref. Further development of Dynamic Testing 2 – Phase 2 (NewDDT2-3 PP/40115457/MB – Guidelines on Statistical Testing for logic or Software Elements used in Nuclear Safety Related Systems.) • Static analysis The feasibility and full extent of the application of MALPAS analysis to the Protection System application code needs to be confirmed. To date the RP has reported that it has undertaken a feasibility study which indicates that the technique is viable but the RP has stated that further work is required to ensure the technique is scaleable and applicable to the full scope of the PS application code. • Compiler validation. With regard to compiler validation, ONR is aware that the RP is considering a number of options from a Sizewell B type Source to Code Comparison to running a compiler		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

PROTECTION SYSTEM INDEPENDENT CONFIDENCE BUILDING MEASURES

GI-UKEPR-CI-02 REVISION 2

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-02**	**GDA Issue Action Reference**	**GI-UKEPR-CI-02.A1**
	validation test suite (along the lines of an approach developed by NPL). The ICBM approach (Scope, depth and rigour) for each of the above needs to be fully defined before ONR can come to a conclusion on the adequacy of the safety case for the Protection System. Currently there are too many elements that have not been fully defined and as a result further work will be required to confirm the adequacy of the proposed ICBMs, or alternative means agreed by the Regulator. For further guidance see also T16.TO2.09 in Annex 6 and T15.TO2.07, T15.TO2.18 and T15.TO2.19 in Annex 5.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
CLAIMS, ARGUMENTS, EVIDENCE TRAIL
GI-UKEPR-CI-03 REVISION 2

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-03**	**GDA Issue Action Reference**	**GI-UKEPR-CI-03.A1**
GDA Issue	The quality of the assessed Claims, Arguments and Evidence supporting documentation provided by EDF and AREVA requires revision and improvement.		
GDA Issue Action	The CAE trail documentation provided by EDF and AREVA requires revision and improvement. EDF and AREVA to revise and improve the CAE trail documentation. In particular to: • review the UK EPR PCSR C&I sections and ensure that a clear CAE trail is provided for all key claims; • identify the evidence and related argument which demonstrates satisfaction of each of the ONR C&I SAPs. For more guidance see: T13.TO1.01, T13.TO1.02, T13.TO1.03 (including all TOs referenced in the TO Table) and T13.TO2.01 to T13.TO2.43 in Annex 3; T16.TO2.27 in Annex 6; T17.TO2.26 in Annex 7; and T18.TO2.08 in Annex 8. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
SMART DEVICES
GI-UKEPR-CI-04 REVISION 1

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	Electrical Engineering		
GDA Issue Reference	**GI-UKEPR-CI-04**	**GDA Issue Action Reference**	**GI-UKEPR-CI-04.A1**
GDA Issue	EDF and AREVA have yet to define a methodology to be used to qualify Smart Devices for Nuclear Safety functions.		
GDA Issue Action	EDF and AREVA to define the methodology to be used to qualify smart devices used in the implementation of nuclear safety functions and produce examples of the implementation of the methodology for two smart devices, one from Class 1 and one from Class 2. EDF and AREVA have yet to define a methodology to be used to qualify smart devices for use in Nuclear Safety functions. A significant programme of work may be required to justify equipment that incorporates smart devices. This topic has been discussed with EDF and AREVA, and a position paper provided. However, further definition of the methodology and examples of its implementation are required. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
OBSOLESCENCE OF SPPA T2000 PLATFORM
GI-UKEPR-CI-05 REVISION 2

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-05**	**GDA Issue Action Reference**	**GI-UKEPR-CI-05.A1**
GDA Issue	The EDF and AREVA C&I architecture includes systems based upon SPPA T2000 (Siemens S5 based), but this platform is believed to be obsolete and will not be available for UK EPR.		
GDA Issue Action	The EDF and AREVA C&I architecture includes systems based upon SPPA T2000 (Siemens S5 based), but this platform is believed to be obsolete and will not be available for UK EPR. The RP needs to define the platform that will be provided for the UK EPR and submit a Basis of Safety Case that fully addresses the change from the SPPA T2000 (Siemens S5 based) to the proposed system. A Basis of Safety Case in this context is expected, amongst others, to: • define the safety principles and standards (i.e. company, national and international) that are to be adopted for the replacement systems (i.e. incorporating the replacement platform); • justify how these safety principles and standards will be complied with at each step of the development and deployment of the replacement systems; • justify how functional and performance requirements will be satisfied; • demonstrate conformance with relevant ONR SAPs; • provide a full analysis of the impact of the replacement platform on the overall C&I design; and • provide precise details of the change and demonstrate that the systems (covering all new components, tools and methods, etc.) are fit for purpose. It is understood that the proposed system is likely to be based on the Siemens S7 product and that the main impact of the change is the use of a different processor board. This will have an impact on the current SPPA T2000 (Siemens S5 based) based safety demonstration which may affect, amongst others, ability to reuse application code already developed , tool qualification, test records and proven in use arguments etc. At first sight this may appear to be a site licensing issue but our reason for including it as a GDA Issue is because of the profound importance that the platform selection of the SAS and PAS has on the safety of the EPR. In particular the diversity of these systems with the TXS is fundamental and therefore our view that the selection criteria for a replacement platform technology should be reviewed as a part of the GDA process. For further guidance see also T15.TO1.45 in Annex 5 and T18.TO1.04 in Annex 8. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
ISSUES ARISING FROM RI02
GI-UKEPR-CI-06 REVISION 3

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A1**
GDA Issue	In response to our assessment, EDF and AREVA have agreed architecture changes, categorisation changes and have committed to develop a programme of Independent Confidence Building Measures to support the EPR C&I safety case. The nine actions under this GDA issue are concerned with C&I architecture and related matters.		
GDA Issue Action	EDF and AREVA to provide a comprehensive justification of diversity and independence between NCSS/PS, NCSS/SAS-PAS and PS/SAS-PAS commensurate with the level of design for a pre-construction safety report. One of the C&I architectural changes introduced in response to RI02 was the addition of a Non-Computerised Safety System as a backup to the computer- based Safety Automation System/Process Automation System and the Protection System. The EDF and AREVA safety case claims diversity and independence between each of these systems, however, this claim has not been fully substantiated. The regulator expects that this detailed diversity analysis will draw on appropriate standards and guidance. It is also expected that this analysis will be rigorous and ensure all common components are identified together with argumentation as to why any such components identified do not have the potential to induce Common Cause Failure of the identified systems. Where final detailed design information is not available, but which is identified as having a potential impact on the diversity analysis, this should be noted and ONR will use the vehicle of an assessment finding to track the gathering of this evidence from a future licensee. For further guidance see also T16.TO2.21 in Annex 6, T18.TO1.03, T18.TO1.04 and T18.TO2.09 in Annex 8 and T20.A1.2.3 and T20.A1.3.4 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
ISSUES ARISING FROM RI02
GI-UKEPR-CI-06 REVISION 3

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	**PSA**		
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A2**
GDA Issue Action	EDF and AREVA to provide a justification of the reliability figures used for each of the protection systems when claimed independently and in combination. The response should include consideration of systematic and hardware failures, and compliance with appropriate guidance and standards. The EDF and AREVA safety case makes a claim of $1x10^{-4}$ probability of failure on demand (pfd) for the Class 1 Protection System (PS), $1x10^{-2}$ pfd for the Safety Automation System (SAS) and $1x10^{-3}$ pfd for the Non-Computerised Safety System (NCSS). However, a justification for each of these figures needs to be provided, for example, drawing on appropriate international standards (covering random and systematic failures). In addition, for the claims to be used in a way which allows their multiplication, additional argumentation will be required (e.g. claims of independence and diversity which will need to be substantiated) – see GI-UKEPR-CI-06.A1. For further guidance see also T16.TO2.21 in Annex 6, and T20.A1.4.1 and T20.A1.4.2 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
ISSUES ARISING FROM RI02
GI-UKEPR-CI-06 REVISION 3

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A3**
GDA Issue Action	EDF and AREVA to provide a justification of the approach to be used to demonstrate the adequacy of computer based systems important to safety including identification of production excellence and independent confidence building activities. SAP ESS.27 requires that where a safety system's reliability is significantly dependent upon the performance of computer software, the establishment of and compliance with appropriate standards and practices throughout the software development life-cycle should be made, commensurate with the level of reliability required, by a demonstration of 'production excellence' and 'confidence-building' measures. Note that the Protection System's independent confidence building measures are to be addressed under GI-UKEPR-CI-02. For further guidance see also T20.A1.4.1.a in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
ISSUES ARISING FROM RI02
GI-UKEPR-CI-06 REVISION 3

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A4**
GDA Issue Action	EDF and AREVA to provide a revised document NLN-F DC 193 'Protection System – System Description' to reflect the current design and to provide full justification for the design, including the justification of hardwired links to the PS. The assessed revision of NLN-F DC 193 does not reflect agreed architectural changes and does not provide justification for all the hardwired links from lower class systems to the Class 1 Protection System (noting that there may be detailed implementation issues which cannot be fully addressed under GDA). For further guidance see also T17.TO1.04 in Annex 7, T20.A2.2.1 and T20.A2.2.3 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
ISSUES ARISING FROM RI02
GI-UKEPR-CI-06 REVISION 3

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A5**
GDA Issue Action	EDF and AREVA to provide detailed substantiation of independence between Process Instrumentation and Control System (PICS) Class 3 system and the Safety Actuation System (SAS) Class 2 system. There are data highway based communications from the Class 3 to the Class 2 system and EDF and AREVA are required to provide detailed substantiation that failure of the lower class system cannot compromise operation of the higher class system. For further guidance see also T20.A2.3.2 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
ISSUES ARISING FROM RI02
GI-UKEPR-CI-06 REVISION 3

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A6**
GDA Issue Action	EDF and AREVA to provide detailed substantiation of the Class 1 control and display facilities to be provided in the MCR and RSS. A Basis of Safety Case for the Class 1 control and display system to be provided and also a justification in terms of the functional coverage of this system. In response to our assessment a number of C&I architectural changes were introduced to eliminate network communications from lower class systems to the Class 1 protection system, and one such change was the introduction of Class 1 control and display panels in the Main Control Room and the Remote Shutdown Station. EDF and AREVA has indicated that the arrangements will be enhanced by provision of a Qualified Display System (QDS). However, the proposed technical solution, and the scope of the displays/controls needs to be confirmed. For further guidance see also: T16.TO1.03 in Annex 6; T17.TO1.14, T17.TO1.15 and T17.TO2.16 in Annex 7; and T20.A3.6 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
ISSUES ARISING FROM RI02
GI-UKEPR-CI-06 REVISION 3

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A7**
GDA Issue Action	EDF and AREVA to justify why it is not reasonably practicable for the SICS controls to be in a functional state during normal operation. Normal control is through use of the PICS controls with a switch mechanism used to activate the SICS controls on detection of PICS failure. EDF and AREVA is to describe the arrangements used for this changeover including detection of PICS failure. The SICS displays remain active but the audible alarms are muted. The description to be provided by EDF and AREVA will include an argument as to why leaving the SICS controls inactive until needed following PICS failure is preferable to having them active. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
ISSUES ARISING FROM RI02
GI-UKEPR-CI-06 REVISION 3

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A8**
GDA Issue Action	EDF and AREVA to provide evidence, for those functions important to safety which use the Class 3 Terminal bus and/or Plant bus, that end-to-end response time requirements are achievable by design. EDF and AREVA have yet to provide adequate substantiation to confirm that performance is guaranteed by design for those functions which use the Class 3 Terminal bus and/or Plant bus with respect to the end-to-end response time. For further guidance see also T20.A5.4 and T20.A5.5 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT
GDA ISSUE
ISSUES ARISING FROM RI02
GI-UKEPR-CI-06 REVISION 3

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	**PSA**		
GDA Issue Reference	**GI-UKEPR-CI-06**	**GDA Issue Action Reference**	**GI-UKEPR-CI-06.A9**
GDA Issue Action	EDF and AREVA to provide detailed substantiation for the probabilistic claims for any C&I components used by more than one line of protection e.g. sensors, smart devices, PIPS, PACS (response to include consideration of the potential for common mode failure as a result of the use of these components). A comprehensive analysis should be provided by EDF and AREVA to address the potential for Common Cause Failure due to the use of common components in different nominally diverse systems. Also to address the use of items used to provide inputs to more than one line of protection, such as PIPS, and items which combine outputs from nominally diverse/independent systems such as the PACS. For further guidance see also: T17.TO2.07, T17.TO2.08 and T17.TO2.28 in Annex 7; T18.TO1.02, T18.TO1.05 and T18.TO2.06 in Annex 8; T20.A1.3.1 and T20.A1.3.5 in Annex 9. With agreement from the Regulator this action may be completed by alternative means.		

Annex 3

C&I SAP Conformance and Adequacy of PCSR Review for – TSC Summary[3]

Note this information has been imported from a TSC report (Ref. 28) and the formatting of the TSC report has been retained.

[3] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 3

A Annex: TSC Task Summary: C&I SAP Conformance and Adequacy of PCSR Review for UKEPR

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of C&I SAP conformance and adequacy of PCSR for the UK EPR reactor design (TSC Task 11-13).

The Requesting Party (RP) for the UK EPR reactor design is EDF and AREVA.

The aim of the Task 13 review has been to gain confidence that EDF and AREVA have adequate evidence to demonstrate that the claims and arguments presented in the PCSR are adequately substantiated, and that the design of the C&I for the UK EPR can be shown to be in conformance with the HSE/ND C&I SAPs or that adequate justifications have been provided for any non-conformances.

The main areas of activity covered in the Task 13 review were:

- the EDF and AREVA demonstration of Conformance with the HSE/ND C&I Safety Assessment Principles (SAP), including the EDF and AREVA response to RO-UKEPR-62 Action A2;
- the adequacy of the Pre-Construction Safety Report (PCSR) with respect to a clear Claims/Arguments/Evidence (CAE) trail, including EDF and AREVA's response to RO-UKEPR-62 Action A1;
- the safety case for selected sample Sensors;
- PCSR updates received during the period of the Step 3 (TSC Tasks 1 to 3), and
- Technical Observations raised by Step 3 Task 1 to 3 and Step 4 Task 11 and 12 Technical Queries in relation to Claims and Arguments for conformance with HSE/ND C&I SAPs.

This Task 13 review follows on from the review of Claims and Argumentation in support of conformance with HSE/ND C&I SAPs carried out in preliminary Step 3 activities (TSC Tasks 1 to 3). In the absence of a clearly documented demonstration of SAP conformance during Step 3, the TSC reviewed the June 2008 version of the UK EPR PCSR in an attempt to identify Claims and Arguments relating to a demonstration of conformance with the HSE/ND C&I SAPs and to identify links to supporting evidence for review during Step 4. During Steps 3 Task 1 to 3 the Claims/Argumentation and identification of supporting evidence review was concluded for 63 First and Second Tier SAPs (identified by HSE/ND for Step 3 review) of the 84 HSE/ND C&I SAPs

The Task 11 and 12 review activity has covered the Claims and Arguments for the remaining 21 Third Tier SAPs not previously addressed in Step 3 and the Task 13 activity covered the sampled review of evidence identified by EDF and AREVA that supports the Claims and Arguments in relation to conformance with all 84 HSE/ND C&I SAPs. EDF and AREVA presented CAE documentation to support a demonstration of conformance to HSE/ND C&I SAPs during Step 4.

The scope of the evidence that is specific to UK EPR is defined by EDF and AREVA in *"UK EPR CONTROL AND INSTRUMENTATION (C&I) – SCOPE OF GDA"* (letter ND(NII)EPR00686N). The review of the evidence in support of the RP's Claims-Argument-Evidence information (CAE Trail) and the review of Sensors are consistent with this scoping letter.

Annex 3

A total of 47 technical observations resulting from the review have been raised. These technical observations (TO) have been designated TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher – 3 of these have been designated TO1 and 44 have been designated TO2.

SAP Conformance and Adequacy of PCSR

During GDA Step 2, HSE/ND raised a number of Observations against the EDF and AREVA 'Claims' made in document *'UKEPR-0005-001 Issue 00 'COMPARISON OF EPR DESIGN WITH HSE/NII* SAPs'. The adequacy of the Claims-Argument-Evidence to support the EDF and AREVA demonstration of conformance with HSE/ND C&I SAPs is addressed by Step 3 Tasks 1-3 and Step 4 Tasks 11-13. The technical aspects of the Observations raised by HSE/ND during Step 2 are being addressed by the appropriate TSC Step 4 Tasks and the status of these Observations is reported in the respective TSC Step 4 Task reports.

The reviews of Claims, Arguments and identification of Evidence carried out during TSC Step 3 Tasks 1 - 3 and Step 4 Task 11 and 12 revealed areas for improvement (AFI) in the demonstration of SAP conformance presented by EDF and AREVA. During the conduct of the Step 3 Tasks 1-3 reviews the AFI were raised as technical queries (TQ) and were included as 'SAP Assessment' related Step 3 observations in the HSE/ND GDA Step 3 report. During the conduct of the Step 4 Task 11 and 12 reviews the AFI were raised as a single technical query (TQ). These have either been cleared (i.e. transferred to other tasks) or resolved (no further action required).

The lack of a clear CAE Trail within the PCSR to demonstrate conformance to HSE/ND C&I SAPs resulted in a Regulatory Observation (RO-UKEPR-62) being raised with EDF and AREVA. RO-UKEPR-62 has two actions:

RO-UKEPR-62 A.1 - ***The Requesting Party is required to review and revise the UK EPR PCSR C&I sections so that a clear claims-argument evidence trail exists within the document for all claims.***

The initial EDF and AREVA response to this action, '*RO-UK EPR -62 – ACTION A1 PCSR I&C Claims, Arguments and Evidence (CAE) Report on the CAE Approach,'* was received under letter ND(NII)EPR618N dated 27 October 2010. Review comments on this CAE Approach were provided via a technical query issued by the HSE/ND (TQ-EPR-1364). Although the general structure of the approach was generally acceptable, the main conclusions were that it effectively replicated the SAP based CAE Trail in the EDF and AREVA document PELL-F DC 9 (see RO-UKEPR-62 action A2 below) and neither the derivation of High Level Claims and Key Claims nor their location within the PCSR was clearly identified. It was not clear how this initial part response to RO-UKEPR-62 A.1 demonstrated that '*a clear claims argument evidence trail exists within the document (PCSR)*' as required by RO-UKEPR-62 A1.

The second EDF and AREVA response '*RO-UK EPR -62 – ACTION A1 PCSR I&C Claims, Arguments and Evidence (CAE) Interim Report*' received under cover of letter EPR00707N dated 17 December 2010 took cognisance of TQ-EPR-1364. However, there remain a number of similarities to the PELL-F DC 9 CAE Trail and there is no clearly defined link to the UK EPR C&I Requirements Specification, or other applicable source, for the derivation of Claims made against the C&I design. Also, the wording of many of the Sub-Claims appears to be taken directly from the HSE/ND SAPs whereas these Claims (High Level, Key and Sub Claims) should be generated by the RP independent of the SAPs. A Step 4 technical observation (TO) (T13.TO1.01) has been raised to address these AFI.

Annex 3

RO-UKEPR-62 A.2 - *The Requesting Party is required to identify the evidence and related argument which demonstrates satisfaction of each of the HSE C&I SAPs.*

Following review of the initial EDF and AREVA response to RO-UKEPR-62 A.2 received under cover of letter ND(NII)00360R dated 15 April 2010, EDF and AREVA provided a more detailed and focused SAP conformance document (PELL-F DC 9) that was used as the CAE Trail against which the sampled review of evidence was undertaken. A key aim of this review has been to gain confidence that an adequate level of conformance against the HSE/ND C&I SAPs is demonstrated through the EDF and AREVA CAE Trail.

The 84 SAPs intended to be reviewed by Task 13 were divided into 4 Phases to prioritise the review process. Specific SAPs were apportioned to a number of other TSC Step 4 Tasks for detailed sampled evidence review in the context of these Tasks. The CAE Trail documents were delivered by EDF and AREVA in three stages to address Phase1, Phase 2, and then Phases 3 & 4 SAPs.

An initial review has been undertaken of the CAE Trails for all 84 Phase 1, 2, 3 and 4 C&I SAPs to determine the level of adequacy based on the coverage of SAP requirements, adequacy of argument, relation to any areas for improvement identified in earlier reviews, and appropriateness of the evidence identified by EDF and AREVA.

From this initial review of these 84 SAPs, 16 have been declared Out of Scope of GDA or not relevant to C&I by EDF and AREVA. For the remaining 68 in scope SAPs, this initial high level review of the CAE Trails indicates that 38 of the CAE Trails have significant areas for improvement. However, most CAE Trails have a number of areas for improvement and a Step 4 technical observation (T13.TO1.02) has been raised by TSC Task 13 to address these. T13.TO1.02 is supported by 43 further Step 4 Task 13 technical observations (T13.TO2.01 to T13.TO2.43).

Due to the timing of issue of the CAE Trail documents by EDF and AREVA, it was only possible to complete a sampled evidence review of the twenty four Phase 1 and two Phase 2 SAPs within the timeframe of the GDA Step 4 review. The sampled review of evidence against the CAE Trails for these SAPs concluded that EDF and AREVA has demonstrated a 'broadly acceptable' level of SAP conformance for 6 SAPs; these included 4 Phase 1 and the 2 Phase 2 SAPs. However, there remain some areas for improvement associated with these 6 SAPs that need to be addressed. It was also concluded that EDF and AREVA did not demonstrate an 'acceptable' level of SAP conformance for 19 SAPs. One SAP (ESR.7 – Communications Systems) was declared Out of Scope of GDA by EDF and AREVA. The SAPs sampled evidence reviews have identified areas for improvement and a technical observation (TO) (T13.TO1.03) has been raised by TSC Task 13 to address these. T13.TO1.03 is supported by 92 technical observations raised by TSC Step 4 Tasks 14-18 during the sample review of evidence against the CAE Trails. The specific context of the supporting TOs is presented in a matrix *'NII GDA Technical Review – C&I - Step 4 Tasks UKEPR CAE Trail & Evidence Review Matrix, 37194/64262V Issue 1.0'*.

Sampled supporting evidence against the CAE Trails was reviewed for the following SAPs:

Phase 1: ECS.1, ECS.2, ECS.3, EQU.1, EDR.1, EDR.2, EDR.3, EDR.4, ERL.3, EMT.7, ESS.1, ESS.2, ESS.3, ESS.7, ESS.8, ESS.18, ESS.21, ESS.23, ESS.27, ESR.1, ESR.3, ESR.5, ESR.7, ERC.2.

Phase 2: EKP.3 and ESS.15.

Annex 3

Sensor Review

A review of Sensors (excluding Smart sensors that use microprocessors) used within the UK EPR C&I design was undertaken. This covered In-core, Ex-core and Process Instrumentation sensors/detectors. Detailed design or manufacturing of process sensors is out of scope for GDA. The GDA Scope for Process Sensors is set out in letters ND(NII)EPR00376N and ND(NII)EPR00686N and is limited to examples of instrumentation requirement specifications for the UKEPR and examples of qualification reports or qualification programmes related to the Flamanville 3 (FA3) project, to be provided by EDF and AREVA. These 'examples' were further requested by Technical Query (TQ) TQ-EPR-1283 but were not received in the timescale of the review.

The review concentrated (as agreed with HSE/ND) on two In-Core Instrumentation systems; the Self Powered Neutron Detectors (SPND) and the Core Outlet Thermocouple (COT) system. This decision was driven by the availability of specification information and importance of these two systems to reactor protection. A review of the SPND System Specification and the In-core Reactor Instrumentation System (RIS) System Design Manual (SDM) was conducted against third tier standard IEC 61468:2000 '*Nuclear Power Plants – In-core instrumentation – Characteristics and test methods of self-powered neutron detectors (SPND)*'. This review has shown that some design requirements specified in IEC 61468:2000 have been addressed in the System Specification documents and RIS SDM. The latter documents have been reviewed but no clear supporting evidence was identified within them to demonstrate conformance with many areas of IEC 61468:2000. A TO (T13.TO2.44) has been raised to address these areas for improvement.

A similar review of the COT System Specification and the RIS SDM was conducted against third tier standard IEC 60737:2010 '*Nuclear Power Plants - Instrumentation Important to Safety - Temperature Sensors (in-core and primary coolant) - Characteristics and test methods*'. Again, this review has shown that some design requirements specified in IEC 60737:2010 have been addressed in the System Specification documents and RIS SDM reviewed but no clear supporting evidence was identified within these documents to demonstrate conformance with many areas of IEC 60737:2010. In both cases, further detailed evidence is needed as the specific design and procurement progresses. A TO (T13.TO2.44) has been raised to address these areas for improvement.

A technical query (TQ) (TQ-EPR-1283) was raised by HSE/ND requesting information on IEC standards used or required to be used in relation to sensors (In-core, Ex-core and Process) and demonstration of compliance with them; no response was provided within the timescale for this review. Additionally, evidence of Sensor Qualification for normal and emergency operating conditions was requested but was not provided within the timescale of the review. A TO (T13.TO2.44) has been raised to address these areas for improvement.

PCSR Update Impact Review

The April 2008 issue 1 of the UK EPR PCSR, which was used during Step 3 task 1-3 activity, was updated on two occasions; June 2009 and November 2009. After each update a review was conducted of the C&I sections to determine the impact of the update on the outcome of preliminary activities. The conclusions of these reviews are presented below:

Annex 3

The review of the June 2009 Issue 2 of the PCSR concluded that it has not introduced significant changes to the C&I architecture, nor significant improvements to the safety argumentation presented in the PCSR, compared to the April 2008 Issue 1. In particular, major observations remained over:

- the reliability claims for the Teleperm XS and SPPA-T2000 platforms,
- the platform diversity claims and reliance on two computer based platforms only;
- inputs into the Class 1 system from non-Class 1 sources,
- absence of common cause failure analysis,
- absence of architectural requirements,
- absence of safety group definitions, and
- absence of application of single failure criterion to safety group members.

The Issue 2 June 2009 PCSR had no discernable impact on the preliminary activities conducted under GDA Step 3 TSC Tasks 1 to 3, Task 7 and Task 8.

The review of the November 2009 Issue 3 of the PCSR concluded that the C&I sub-chapters and Appendices were sufficiently similar to those in the June 2009 issue to be considered to be identical. As such, the November 2009 issue had no impact on any GDA Step 3 review work by the TSC Tasks previously undertaken.

Technical Observations

During the conduct of the Step 3 Tasks 1-3 reviews of the Claims and Arguments and identification of evidence the AFI were raised as technical queries (TQ) and were included as 'SAP Assessment' related Step 3 observations in the HSE/ND GDA Step 3 report. During the conduct of the Step 4 Task 11 and 12 reviews the AFI were raised as a single technical query (TQ). These have either been cleared (i.e. transferred to other tasks) or resolved (no further action required). There are no outstanding Step 3 Task 1-3 or Step 4 Tasks 11 and 12 TQs or TOs.

A review of RO-UKEPR-62 A.1 and A.2 responses and In-Core Instrumentation sensors has been performed by Task 13. A total of 47 technical observations resulting from this review have been raised by Task 13; 3 of these observations have been designated as TO1 (T13.TO1.01 to T13.TO1.03). However, 43 of these technical observations, designate TO2 (T13.TO2.01 to T13.TO2.43), have been raised by Task 13 that support the TO raised by Task 13 (T13.TO1.02) against the CAE Trail presented as the basis of the EDF and AREVA demonstration of conformance with the HSE/ND C&I SAPs (i.e. response to RO-UKEPR-62 A.2). Additionally, 92 technical observations have been raised by other TSC Step 4 Tasks 14 to 18 that support the TO raised by Task 13 (T13.TO1.03) against the sampled review of evidence from the CAE Trails that the RP claims support SAP conformance. These other Step 4 TSC Task observations are reported in the applicable Step 4 TSC Task reports. One observation has been designated as TO2 (T13.TO2.44) against Sensors (In-Core, Ex-Core and Process).

Technical Observations designated TO1:

The three TO1 technical observations relating to RO-UKEPR-62 are as follows:

Annex 3

T13.T01.01 – Although the initial part responses to RO-UKEPR-62 A.1; *'RO-UK EPR -62 – ACTION A1 PCSR I&C Claims, Arguments and Evidence (CAE) Report on the CAE Approach,'* received under letter ND(NII)EPR618N dated 27 October 2010 and '*RO-UK EPR -62 – ACTION A1 PCSR I&C Claims, Arguments and Evidence (CAE) Interim Report*' received under cover of letter EPR00707N dated 17 December 2010, demonstrate a sound approach methodology, the designer or future operator/licensee is requested to address the following in further developing this methodology and its output to ensure that a clear claims-argument evidence trail exists within the document for all claims:

a. provide a clear explanation or demonstration of how High Level and Key Claims are derived from appropriate sources, such as C&I Design Requirements Specification, Criteria or Principles, or other appropriate sources.

b. clearly identify the location of the Claims and Arguments within the PCSR, and identification of appropriate supporting Evidence.

c. The wording of the Claims, particularly the Sub-Claims should be derived independently from the SAPs and relate to the designer or future operator/licensee's key claims such as satisfaction of safety principles/criteria.

T13.T01.02 – Although the C&I SAP CAE Trail in document PELL-F DC 9 has developed as an acceptable methodology for the demonstration of conformance to the HSE/ND C&I SAPs, there are still significant areas for improvement (AFI) in the presented Argument and identified Evidence for a large number of SAPs. The AFI relating to the CAE Trails for HSE/ND C&I SAPs are addressed in 43 Technical Observations (TO) (T13.T02.01 to T13.T02.43). The designer or future operator/licensee is requested to take all AFI in the 43 supporting TOs into account in further development of a robust demonstration of conformance with HSE/ND C&I SAPs.

T13.T01.03 – Following sampled evidence review against the CAE Trails, TSC Step 4 Tasks 14 to 18 identified areas for improvement (AFI) and raised 89 TOs, as listed in the Table below that are reported in detail in the respective TSC Task reports. The designer or future operator/licensee is requested to take all AFI in these TOs raised by TSC Tasks 14 to 18 into account in further development of a robust demonstration of conformance with HSE/ND C&I SAPs.

SAP	Title	Task 14	Task 15	Task 16	Task 17	Task 18	Task 20
ECS.1	Safety categorisation and standards.				T17.T01.01.a T17.T01.01.b		
ECS.2	Safety classification of structures, systems and components.				T17.T01.01a T17.T01.01.b T17.T01.02a T17.T01.02.b T17.T01.02.c T17.T01.04 T17.T02.03		T20.A2.3.2
ECS.3	Standards.	T14.T01.01					

Annex 3

SAP	Title	Task 14	Task 15	Task 16	Task 17	Task 18	Task 20
		T14.T01.02 T14.T02.01					
EQU.1	Qualification procedures.	T14.T02.05	T15.T02.28 T15.T02.29 T15.T02.30 T15.T02.31 T15.T02.32 T15.T02.41	T16.T02.01 T16.T02.25			
EDR.1	Failure to safety.		T15.T02.49 T15.T02.50 T15.T02.62	T16.T02.22	T17.T01.04 T17.T02.05 T17.T02.06		T20.A2.2.1
EDR.2	Redundancy, diversity and segregation.		T15.T01.55	T16.T02.03 T16.T02.23	T17.T02.08	T18.T02.01 T18.T02.03 T18.T02.07	T20.A1.2.4 T20.A1.3.1 T20.A1.3.2 T20.A1.3.3 T20.A1.3.4 T20.A1.4.1 T20.A2.3.4
EDR.3	Common cause failure.		T15.T02.51 T15.T02.54 T15.T02.57 T15.T02.58	T16.T02.04 T16.T02.24	T17.T01.01.b	T18.T01.02	
EDR.4	Single failure criterion.				T17.T02.08 T17.T02.09a T17.T02.09b		T20.A1.3.1
ERL.3	Engineered safety features.				T17.T02.10		
EMT.7	Functional testing.			T16.T02.05 T16.T02.26			
ESS.1	Requirement for safety systems.				T17.01.02a		
ESS.2	Determination of safety system requirements.						
ESS.3	Monitoring of plant safety.				T17.T01.01a T17.T01.02a T17.T01.14 T17.T01.15		

Annex 3

SAP	Title	Task 14	Task 15	Task 16	Task 17	Task 18	Task 20
					T17.T02.16		
ESS.7	Diversity in the detection of fault sequences.				T17.T01.02a T17.T02.17		
ESS.8	Automatic initiation.						
ESS.18	Failure independence.			T16.T02.06	T17.T01.04	T18.T02.01 T18.T02.07	T20.A1.3.1 T20.A2.3.2
ESS.21	Reliability.	T14.T01.02		T16.T02.18 T16.T02.07	T17.T01.04 T17.T02.05 T17.T02.06 T17.T02.19		
ESS.23	Allowance for unavailability of equipment.		T15.T02.52	T16.T02.08	T17.T02.20		
ESS.27	Computer based safety systems.	T14.T02.06	T15.T01.18 T15.T01.38 T15.T02.05 T15.T02.53 T15.T02.59 T15.T02.60	T16.T01.01 T16.T02.09			
ESR.1	Provision in control rooms and other locations.				T17.T01.11 T17.T01.14 T17.T01.15		
ESR.3	Provision of controls.		T15.T02.62		T17.T01.01a T17.T01.14 T17.T02.21		T20.A4.6.2
ESR.5	Standards for computer based equipment.	T14.T01.02 T14.T02.02 T14.T02.03 T14.T02.04	T15.T01.46 T15.T02.60	T16.T02.27 T16.T02.28 T16.T02.29 T16.T02.30 T16.T02.31			
ESR.7	Communications systems.				T17.T02.22		
ERC.2	Shutdown systems.					T18.T02.03 T18.T02.06	

Annex 3

SAP	Title	Task 14	Task 15	Task 16	Task 17	Task 18	Task 20
EKP.3	Defence in depth.				T17.T01.01.a		
ESS.15	Alteration of configuration, operational logic or associated data.		T15.T02.61				

Technical Observation designated TO2:

T13.T02.01 - From the review of the CAE Trail for ECS.3 the following area for improvement is raised:

- There is reference to System Description reports but no indication of specific document identification. Also, the third point against guidance paragraph 159 states that *'Evidence will be provided that standards*.....' with no indication as to what form that evidence will take. The designer or future operator/licensee is requested to ensure that appropriate specific document references are included in the CAE Trails.

T13.T02.02 - From the review of the CAE Trail for EDR.2 the following areas for improvement are raised:

- An argument is put forward for Redundancy in the PICS with no supporting evidence. The designer or future operator/licensee is requested to ensure that appropriate specific document references to support the argument for redundancy in the PICS are included in the CAE Trails.

- There is reference to Reliability Analyses for the SAS & PAS, but not for the F1A PS. The designer or future operator/licensee is requested to ensure that reliability analyses are identified for the PS and included in the CAE Trail.

T13.T02.03 - From the review of the CAE Trail for EDR.4 the following area for improvement is raised:

- The response to TQ-EPR-315 quotes the PSA as modelling assumed single failures, yet the PSA (NEPS-F DC 355 Rev B) is not cited as evidence to this SAP. The designer or future operator/licensee is requested to ensure that the appropriateness of NEPS-F DC 355 to support this SAP is reassessed and included in the CAE Trail if relevant.

T13.T02.04 - From the review of the CAE Trail for ERL.3 the following areas for improvement are raised:

- The evidence pointed to is all PCSR Sub-chapters, predominantly Sub-chapters 18.1 and 14.7; the latter being the Fault Schedule. A new Fault Schedule (PEPR-F DC 4 B) has been provided and commented on by HSE/ND but is not included here. The designer or future operator/licensee is requested to ensure that the correct reference to the UKEPR Fault Schedule is used in PELL-F DC 9.

- A reference to PCSR Chapter 18.1 Section 3.1.3.1 is *ECEF021855 Revision B1 - ENG 2.21 Procedure: Degree of automation for plant systems*, but this is not listed as evidence. The

Annex 3

designer or future operator/licensee is requested to ensure that where Sections of the PCSR Sub-chapters are quoted in the CAE Trail and they have specific references linked to them, these references are included in the CAE Trail.

- The evidence to support guidance paragraph 180 is 'to be provided', but it has not been stated what is to be provided. The designer or future operator/licensee is requested to ensure that appropriate specific document references are included in the CAE Trails.

T13.T02.05 - From the review of the CAE Trail for EMT.7 the following areas for improvement are raised:

- The argument against paragraph 192 states '*More specific evidence for each F1 system: (PS, PACS, SICS and SAS) is presented* below'. However, no specific evidence is identified to support guidance paragraph 192 requirements except for the Protection System. The designer or future operator/licensee is requested to ensure that appropriate specific evidence is identified and included in the CAE Trail.

- The argument against guidance paragraph 193 states that two examples are provided yet there appears to be only one. The designer or future operator/licensee is requested to ensure that the argument against paragraph 193 is revised to include the correct number of examples.

T13.T02.06 - From the review of the CAE Trail for ESS.1 the following areas for improvement are raised:

- The evidence to demonstrate that safety systems are provided to achieve the requirements of the SAP is the Fault Schedule provided in PCSR Chapter 14.7 introduced in the Nov 09 issue 3 of the PCSR. This has since been superseded with the issue of a new Fault Schedule (PEPR-F DC 4 B) that has not been referenced here. The designer or future operator/licensee is requested to ensure that the correct reference to the UKEPR Fault Schedule is used in PELL-F DC 9.

- The argument and evidence to support the first half of guidance paragraph 336 is quoted as 'to be provided' with no indication of what. The designer or future operator/licensee is requested to ensure that appropriate specific evidence is identified and included in the CAE Trail.

T13.T02.07 - From the review of the CAE Trail for ESS.2 the following area for improvement is raised:

- Section 2.4 of ECECC080669 B is cited as evidence for Defence in Depth Assumptions and Requirements for I&C, but this is a FA3 document. This document does not address the changes to the C&I architecture for UK EPR. A more appropriate (or additional) evidence document for the UK EPR is ECECC100832 A Section 2.1.2 that contains the same Defence-in-Depth information. The designer or future operator/licensee is requested to ensure that appropriate specific UKEPR relevant evidence is identified and included in the CAE Trail.

T13.T02.08 - From the review of the CAE Trail for ESS.3 the following area for improvement is raised:

Annex 3

- PCSR Sub-chapters 7.2 (Section 1.3.3), 7.3 (Section 3) and 18.1 (Section 5.1) are cited as evidence. However, applicable evidence documents that are references from the identified PCSR chapters include:
    - ECECC060019 Revision A. EDF. December 2006. [Main Control Room (KSC [MCR]) System Specification].
    - ECECC070760 B. EDF. December 2008. [System Design Description Main Control Room (KSC [MCR]), Part 5: Control and Instrumentation System (KSC [MCR]) EPR FA3 (Stage 2)].
    - ECECC040729 Revision A. EDF. September 2004 [Process Information and Control System (KIC [PICS]) System Specification.]
    - ECECC080097 Revision B. EDF. December 2008. Process Information and Control System (KIC [PICS]) Part 5: Control and Instrumentation System EPR FA3 (Stage 2).

    The designer or future operator/licensee is requested to ensure that where Sections of the PCSR Sub-chapters are quoted in the CAE Trail and they have specific references linked to them, these references are included in the CAE Trail.

T13.T02.09 - From the review of the CAE Trail for ESS.7 the following areas for improvement are raised:

- The argument states that diversity in detection of fault sequences is covered in PCSR Chapter 7.3; however, the evidence quoted is the Fault Schedule in Chapter 14.7 that has now been replaced with PEPR-F DC 4 B. The designer or future operator/licensee is requested to ensure that the correct reference to the UKEPR Fault Schedule is used in PELL-F DC 9.
- There is no technical evidence presented to support the PCSR on how diversity in detection of fault sequences is implemented. The designer or future operator/licensee is requested to ensure that appropriate specific evidence that demonstrates the implementation of diversity in detection of fault sequences is identified and included in the CAE Trail.
- On diversity in safety system action initiation, the argument and evidence appear to concentrate on Reactor Trip only. The designer or future operator/licensee is requested to ensure that the CAE Trail is reviewed and revised to include diversity in the initiation of all safety system actions.
- The argument quotes PCSR Sub-chapter 7.3. Evidence documents that are references from PCSR Chapter 7.3 but not included in the CAE Trail are:
    - NLE-F DC 38 Rev F - Protection System detailed specification file
    - NLN-F DC 89 A - Protection System - Functional Diagrams.
    - NLE-F DC 59 Revision C. - System Design Manual - Reactor Protection System (RPR), Part 2 – System operation.

Annex 3

The designer or future operator/licensee is requested to ensure that where Sections of the PCSR Sub-chapters are quoted in the CAE Trail and they have specific references linked to them, these references are included in the CAE Trail.

T13.T02.10 - From the review of the CAE Trail for ESS.8 the following areas for improvement are raised:

- The evidence for automatic initiation by the safety systems is given as the Fault Schedule (in the form of PCSR Ch 14.7 rather than PEPR-F DC 4 B). No technical description of the PS that addresses automatic initiation of safety systems has been identified. The designer or future operator/licensee is requested to identify appropriate technical evidence that demonstrated that safety systems are automatically initiated and included this in the CAE Trail.

- The prevention of negating PS action by the PACS electrical switchgear and other functionality of the PACS has not been addressed, neither has evidence been identified to support the first part of guidance paragraph 343 requirements, not even PCSR chapter reference. The response to TQ-EPR-276 provides some information. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to demonstrate the role of the PACS to prevent facility personnel negating safety system action.

- The second part of guidance paragraph 343 mentions permissives and resets and points to PCSR Ch 14 Section 7.3.5 for supporting evidence. There are 7 Sub-chapters and 2 Appendices to Ch 14; it is not clear in which of these Sections 7.3.5 is to be found. Further supporting evidence beyond the PCSR would be expected. The designer or future operator/licensee is requested to ensure that appropriate specific evidence is identified and included in the CAE Trail.

T13.T02.11 - From the review of the CAE Trail for ESS.18 the following areas for improvement are raised:

- The SAP is about faults and hazards (both internal and external). However, there is no reference to the Fault Schedule, FMEA or any Hazard Analysis to demonstrate the architecture design satisfies the SAP requirements. PCSR Chapters 13.1 and 13.2 discuss External and Internal Hazards respectively but they, or any of their supporting references, are not mentioned here. The designer or future operator/licensee is requested to review and revise the argument and evidence to demonstrate that a safety system is not disabled by an internal or external hazard and that appropriate specific evidence is identified and included in the CAE Trail.

- Much of the evidence is Sub-chapters and Appendices of the PCSR and in some cases, such as Appendix 7D in support of the guidance paragraph 352, the wording of the 'argument' comes directly from the 'evidence'. More detailed supporting evidence should be identified that supports the arguments presented in the PCSR, such as NLE-F DC 33 C - Concept for I&C Failure Handling. The designer or future operator/licensee is requested to review and revise the evidence so that appropriate specific evidence is identified and included in the CAE Trail.

T13.T02.12 - From the review of the CAE Trail for ESS.21 the following areas for improvement are raised:

Annex 3

- The first part of this SAP is about avoiding complexity in the design of the safety systems. There is no claim (or argument) that complexity is avoided during the system design process or no demonstration via specific evidence that complexity has been avoided. The argument for the UKEPR implies complexity in the design of safety systems has not been avoided and instead it is intended to justify the complexity of the systems via PE&ICB for software, and a safety demonstration for hardware; hence the link direct to guidance paragraph 355 that only applies when this SAP cannot be achieved. There is no justification presented for why use of complex safety systems is acceptable. Having been directed to guidance paragraph 355, it is stated that the safety demonstration for the complex hardware is yet to be developed, with no indication of timescales. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to include a justification for why use of complex safety systems is acceptable and that appropriate specific evidence is identified and included in the CAE Trail.

- For the SPPA-T2000 it is left to a Self-test coverage analysis (SIE QU633) to demonstrate fail-safe with a module FMEA and a system level reliability study (unreferenced). Individual module FMEAs and the Reliability Analysis for SPPA-T2000 [QU627] are not mentioned in the evidence column. The designer or future operator/licensee is requested to ensure that appropriate specific evidence is identified and included in the CAE Trail.

- There is no argument or evidence to support revealing internal faults for SPPA-T2000. The designer or future operator/licensee is requested to ensure that appropriate specific evidence is identified and included in the CAE Trail.

- For guidance paragraph 356, the use of periodic tests is claimed where faults cannot be revealed until this time. The evidence column states: 'the principles of the periodic tests that will be implemented for the different I&C systems are given in the following evidence'. However, it goes on to say that this will all be addressed during Site Licensing. It is unclear why such evidence as NLE-F DC 34 Rev D - Protection System - Concept for Periodic Tests is not cited here. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to ensure accurate statements and appropriate specific evidence is included in the CAE Trail.

T13.T02.13 - From the review of the CAE Trail for ESS.23 the following areas for improvement are raised:

- The argument mentions, as a general point, that the four-fold redundancy of the design mitigates against unavailability in any one division and more specifically, in determining the safety system provisions for the I&C system, that allowance has been made for the unavailability of equipment due to causes including; testing and maintenance, non-repairable equipment failures and unrevealed failures. However, the evidence cited to support this argument is either Operating Technical Specifications that are out of scope for GDA or evidence to be adapted from that for EMT.6. The designer or future operator/licensee is requested to ensure that appropriate specific evidence is identified that demonstrates that unavailability of equipment has been addressed in determining Safety System provision and that it is included in the CAE Trail.

- Unavailability due to testing and maintenance is quoted in the evidence column as addressed by application of SFC. This is effectively repeating the argument. There should be specific evidence referenced that explains how the removal of equipment for test or maintenance has

Annex 3

been taken into account. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised and appropriate specific evidence is included in the CAE Trail.

- Non-repairable failures and unrevealed failures (guidance paragraph 357 refers) were the subject of TQ-EPR-375 the response to which quoted PCSR Chapter 7 Appendix A Section 3.1.7 as discussing this point. However, this is not provided as part of the argument. The response to TQ-EPR-375 also quoted an FMEA assessment activity as part of a Quantitative assessment process and listed module FMEA that are not referenced. References quoted in the response to TQ-EPR-375 as supporting demonstration that I&C design has been assessed for unavailability in support of this SAP include:

    - NLE-F DC 33 C - Concept for I&C Failure Handling.
    - NLE-F DC 34 Rev D - Protection System - Concept for Periodic Tests.
    - NLTC-G/2008/en/0079 Rev B - TXS Self-monitoring and fail-safe behaviour.

  These are not included in the CAE Trail. The designer or future operator/licensee is requested to ensure that appropriate specific evidence is included in the CAE Trail.

T13.T02.14 - From the review of the CAE Trail for ESS.27 the following areas for improvement are raised:

- For 'Production Excellence' the evidence identified is relevant but there are some evidence documents cited (e.g. NLF-F DC 14 Hardware Qualification) that are hardware based where this is a software based SAP. Also, the argument mentions a System QA Plan as well as a System Quality Plan; there is no System QA Plan listed in the evidence column. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to ensure accurate statements and appropriate specific evidence is included in the CAE Trail.

- For the 'Independent Confidence Building' leg the argument cites much independent checking and surveillance work by parties other than AREVA. However, apart from one CEIDRE inspection report (with no specific document reference) there is no other actual evidence of the independent checks/surveillance carried out. Other evidence is documents that would be checked by ICB or explanation of the ICB process. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to ensure accurate statements and appropriate specific evidence is included in the CAE Trail.

T13.T02.15 - From the review of the CAE Trail for ESR.1 the following areas for improvement are raised:

- Supporting evidence is quoted as PCSR chapters (Sub-chapters 7.2 and 18.1) that effectively provide an argument. More detailed evidence on the MCR, RSS or the PICS/SICS would be expected. References from Sub-chapters 7.2, 7.3 and 7.4 of the PCSR that have not been cited include:

    - ECECC060019 Revision A - Main Control Room (KSC [MCR]) System Specification.
    - ECECC070760 B - System Design Description Main Control Room (KSC [MCR]), Part 5: Control and Instrumentation System (KSC [MCR]) EPR FA3 (Stage 2).
    - ECECC040729 Revision A - Process Information and Control System (KIC [PICS]) System Specification.

Annex 3

- ECECC080097 Revision B - Process Information and Control System (KIC [PICS]) Part 5: Control and Instrumentation System EPR FA3 (Stage 2).

The designer or future operator/licensee is requested to ensure that appropriate specific evidence is included in the CAE Trail.

- ECEF021069 Revision C1 - Sizing of SICS was mentioned in response to TQ-EPR-364 in relation to ESR.1, but has only been cited as evidence to support guidance paragraph 366. The response to TQ-EPR-364 also quoted *'Design documents to provide evidence that the MCR and RSS I&C will provide the described tasks and functions will be available during step 4 when they have been completed'*. Also, in relation to guidance paragraph 366, the PICS is quoted in the argument yet it is only ECEF 021069 'Sizing of SICS' that is cited as evidence. It would be expected that more specific information on the PICS, as well as the SICS, would be identified (see list above). The designer or future operator/licensee is requested to ensure that the CAE Trail is revised and appropriate specific evidence is included in the CAE Trail.

T13.T02.16 - From the review of the CAE Trail for ESR.3 the following areas for improvement are raised:

- No specific evidence has been identified against any argument. More detailed system requirements specifications etc. that set out what controls are provided to 'maintain variables within specified ranges' and why they are considered to be adequate would be expected. The arguments refer to PCSR Sub-chapter 7.4. There are many references listed in the PCSR for Chapter 7.4 Sections 1, 2 and 3 that are not listed here. There is no identified evidence to demonstrate that controls that maintain variables within specified ranges are 'Adequate and Reliable'. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised and appropriate specific evidence is included in the CAE Trail.

- The FMEA referred to in support of demonstration that the controls are reliable is just a 'Methodology' for an FMEA for the TXS based PS. The PS is not relevant to this SAP. The only one of the three systems addressed by the argument (PAS, RCSL and PICS) based on TXS is the RCSL. The PAS and PICS are both based on SPPA-T2000. The SPPA-T2000 reliability analysis (QU627) and module dependability analysis is not cited. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised and appropriate specific evidence is included in the CAE Trail.

T13.T02.17 - From the review of the CAE Trail for ESR.5 the following area for improvement is raised:

- The note in the 'Claim' makes reference to both hardware and software in relation to ESS.27 whereas ESS.27 is only software related. Additionally, the applicable safety related systems are quoted as; PAS, RCSL, SA I&C and PICS. Then only SAS and RCSL are addressed. The SAS seems to have been introduced from nowhere and the PICS, PAS and SA I&C have disappeared. The evidence then cited is for either the SPPA-T2000 or TXS. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to ensure accurate statements and appropriate specific evidence is included in the CAE Trail.

T13.T02.18 - From the review of the CAE Trail for ERC.2 the following areas for improvement are raised:

Annex 3

- No evidence has been identified to support the argument that the EBS/SIS systems can be actuated to perform extra boration when required, by diverse functions within PS and SAS/PAS. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised and appropriate specific evidence is included in the CAE Trail.

- EDF and AREVA claim that guidance paragraph 445 is not applicable to I&C, However, this relates to, for example, situations where the control rods fail to insert on a RT signal from the PS. In this situation an ATWS signal is initiated by the C&I to actuate the EBS and SIS to inject borated water. Some argument and supporting evidence on this should be provided. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised and appropriate specific evidence is included in the CAE Trail.

T13.T02.19 - From the review of the CAE Trail for EKP.3 the following area for improvement is raised:

- The PCSR Chapters 3.1 and 14.7 are cited as providing a discussion on the application of defence in depth with the latter providing the Fault Schedule analysis that provides identification of the functions of the C&I systems to address fault scenarios. It is noted that the Fault Schedule in Chapter 14.7 has now been replaced with PEPR-F DC 4 B. However, this Fault Schedule does not identify the actual C&I systems used to manage a fault condition; it just provides a 'Main Line' function and a 'Diverse Line' function and the Class of system required. The designer or future operator/licensee is requested to ensure that the UKEPR Fault Schedule (PEPR-F DC 4 B) is updated to reflect these comments and to ensure that the statement in the CAE Trail of what the document presents as evidence is correct.

T13.T02.20 – From the review of the CAE Trail for EKP.5 the following areas for improvement are raised:

- The Fault Schedule in Chapter 14.7 of the Nov 2009 PCSR is quoted but it is understood that this has now been replaced with PEPR-F DC 4 B. This also applies to ESS.9. The designer or future operator/licensee is requested to ensure that the correct reference to the UKEPR Fault Schedule is used in PELL-F DC 9.

- Reviewing PEPR-F DC 4 it is noted that the 'Preventative Line' is not identified; it is only the 'Main Line' and 'Diverse Line' identified. Although the Safety Measure (e.g. Reactor Trip) required to deliver a safety function (e.g. Shutdown and remain sub-critical) is identified in the Fault Schedule, there is no mention of the associated C&I System that delivers that safety function. The designer or future operator/licensee is requested to ensure that the UKEPR Fault Schedule is updated to reflect these comments and to ensure that the statement in the CAE Trail of what the document presents as evidence is correct.

- Document ECECC 070637B that list the manual controls and provides the substantiation for their selection, referenced from TQ-EPR-323, has not been listed in the CAE Trail. The designer or future operator/licensee is requested to consider the appropriateness of this document to support conformance with EKP.5 guidance paragraph 146 c) and ensure its inclusion in the CAE Trail if applicable.

- In most cases the evidence cited is sub-chapter and section of the PCSR that might not be most appropriate. Taking 3 examples:

Annex 3

Chapter 7.3 Section 1 is cited but this has numerous References listed in the PCSR that are not mentioned here as supporting evidence; e.g. NLE-F DC 124 Concept for Reactor Trip.

Chapter 7.4 Section 1.0.1 is cited against guidance paragraph 146c), but the wording of the 'Argument' is taken directly from this PCSR Section cited as 'Evidence'.

Chapter 7.3 Section 5.0.1 is cited against guidance paragraphs 146e) and 147 in relation to Severe Accident I&C.

- Ch 7.3 (F1 Systems) does not have a Section 5.
- Ch 7.4 (F2 & NC Systems) does have a Section 5 related to SA I&C.
- Ch 7.4 Section 5.0.1 simply states that the SA I&C 'Limits the radioactive release at the site boundary to an acceptable level and maintains the integrity of the primary and secondary systems'. This is effectively the same as the first line of the 'Argument' in both cases.

The designer or future operator/licensee is requested to review all cited evidence and ensure that the references to supporting evidence are appropriate and correct.

T13.T02.21 - From the review of the CAE Trail for ERL.1 the following areas for improvement are raised:

- Much of the 'Argument' appears to discuss qualification requirements rather than how derivation of reliability claims take account of the various aspects required. Hence Qualification Reports (cited as evidence) would demonstrate that qualification had been carried out, but it is not clear if they provide derivation of reliability claims. The designer or future operator/licensee is requested to ensure clearly referenced evidence is cited in the CAE Trail that provides a derivation of reliability claims.
- 'Reliability Analyses' are cited as evidence for most aspects of the SAP. However, for the final point on 'uncertainties in physical data and design' and against guidance paragraph 176, specific reliability analysis documents are listed for both systems and platforms. It is not clear why specific references have been quoted in these cases but not others. The designer or future operator/licensee is requested to ensure that where specific references are available they are correctly cited against all applicable aspects of the CAE Trail.

T13.T02.22 - From the review of the CAE Trail for ERL.2, EMT.1 and EMT.3 the following area for improvement is raised:

- There needs to be more focused referencing to specific areas within the referenced evidence documents. The designer or future operator/licensee is requested to ensure that references to evidence cited within the CAE Trail are to a specific and appropriate Section rather than a general document reference.

T13.T02.23 - From the review of the CAE Trail for ELO.2 the following area for improvement is raised:

Annex 3

- The evidence description in the CAE Trail calls both NLF-F DC 98 and SY719 4.0 the 'Information Security Plan'. The designer or future operator/licensee is requested to provide clarification as to whether both NLF-F DC 98 and SY719 4.0 are entitled 'Information Security Plan' and ensure correct and accurate referencing of evidence in the CAE Trail.

T13.T02.24 - From the review of the CAE Trail for EHA.10 the following area for improvement is raised:

- The quoting of EMC IEC Standards, 61000-6-2 & 61000-6-4, and other standards/requirements as evidence is inappropriate as the standards provide the requirement, not evidence that the requirement has been met. The designer or future operator/licensee is requested to ensure that where a claim and argument in a CAE Trail cites compliance with an International Standard, the evidence to demonstrate compliance with the standard is cited.

T13.T02.25 - From the review of the CAE Trail for ESS.10 the following areas for improvement are raised:

- More focused/specific document references would be expected. The designer or future operator/licensee is requested to ensure that references to evidence cited within the CAE Trail are to a specific and appropriate Section rather than a general document reference.

- The list of evidence documents includes 'Qualification Documents'. However, the documents referenced in TQ-EPR-359, NLZ-F DC 3 'I&C TXS cabinets qualification program' and NLF-F DC 14 'System qualification program', have not been listed against this SAP. The designer or future operator/licensee is requested to ensure that appropriate specific document references are included in the CAE Trail instead of a generic list of document types.

- The argument against capability exceeding service requirement by a clear margin (para 345) does not appear to address this well. The same generic document list is provided as evidence where specific evidence showing the margin between maximum service requirement and system capability would be expected. The designer or future operator/licensee is requested to ensure that appropriate evidence is identified and included in the CAE Trail that demonstrates that the margin between maximum service requirement and system capability is acceptable.

T13.T02.26 - From the review of the CAE Trail for ESS.11 the following areas for improvement are raised:

- Under 'achieving the specified function' - The PAS is missing from the SPPA-T2000 based systems; it is assumed this would be covered under the QP for SPPA-T2000 cited. There is no evidence identified for the SICS and PACS. Also, under the 'For SICS' the PACS is mentioned instead. The designer or future operator/licensee is requested to ensure that ensure that the CAE Trail is correct and accurately covers the appropriate systems and that appropriate evidence is included for all systems addressed by this SAP.

- Under 'achieving the specified reliability' - Against 'For SICS' it states 'see RAMS for SPPA or TXS'. It has been mentioned in the CAE Trail that the RAMS for PS (NLE-F DM 10032) will not be available until end 2010, but RAMS for TXS or SPPA are not specifically referenced. The designer or future operator/licensee is requested to ensure that specific references to RAMS for TXS and SPPA are included in the CAE Trail.

Annex 3

- The Fault Schedule is cited as PCSR Chapter 14.7 which has been replaced by PEPR-F DC 4 B. It is stated against guidance paragraph 346 that the new fault schedule is currently being produced, whereas it has been issued, and that it allocates safety functions to C&I systems. PEPR-F DC 4 does identify safety functions but it does not identify the specific C&I systems that carry out those function, as required by SAP guidance paragraph 346. The designer or future operator/licensee is requested to ensure that the UKEPR Fault Schedule is updated to identify the specific C&I systems that carry out the safety functions.

T13.T02.27 - From the review of the CAE Trail for ESS.13 the following areas for improvement are raised:

- In relation to b) in the 'Clam', it was identified during the Step 3 review that Sub-chapter 18.1 Section 3.2.2.2 states *'The Process Displays .... provide information on the ....status of actuators*'. However, the evidence column relates to Emergency Operating Procedures (EOPs) being provided at Site Licensing. There is no information or supporting evidence regarding Process Displays and Status of Actuators in the CAE Trail. The designer or future operator/licensee is requested to ensure that appropriate evidence is identified and included in the CAE Trail that demonstrates the confirmation to operating personnel of the status of actuators.

- The SAP paragraph in the second row of the table should be preceded with the paragraph number 349. The designer or future operator/licensee is requested to ensure that the CAE Trail is updated accordingly.

T13.T02.28 - From the review of the CAE Trail for ESS.16 the following area for improvement is raised:

- This SAP is addressed by discussion of continued power supply to the C&I systems and self contained battery back-up supplies within the systems, whereas the SAP relates to maintaining a safe state after a safety system action has put the plant in that safe state. This could be seen, for instance, as no external power required to hold the control rods in the core following initiation of RT by the PS. The designer or future operator/licensee is requested to ensure that the CAE Trail addresses non-dependence on external power supply to maintain a safe state after safety system action.

T13.T02.29 - From the review of the CAE Trail for ESS.20 the following areas for improvement are raised:

- Reference is made to 'Security Plans' with no specific information or delivery dates, but SAP ELO.2 has identified:

    - NLN-F DC 3, Teleperm XS based I&C systems IT Security Plan
    - NLF-F DC 98, Information Security Plan
    - SY719 4.0, Information Security Plan

  It is not clear why these are not referenced here. The designer or future operator/licensee is requested to ensure that specific documents are cited as evidence if available and appropriate.

Annex 3

- There is no document identification or delivery date for the 'Detailed Requirement Specification for Interfaces'. The designer or future operator/licensee is requested to ensure that specific references to evidence documents are included in the CAE Trail.

T13.T02.30 - From the review of the CAE Trail for EMT.5 the following areas for improvement are raised:

- The designer or future operator/licensee is requested to ensure that the evidence cited addresses the requirement to maintain quality and reliability.

- For guidance paragraph 189, the evidence is a RAMS Methodology which is unlikely to demonstrate that in-service testing (Periodic Testing) will detect degradation before loss of Safety Function. The designer or future operator/licensee is requested to ensure evidence is identified and cited in the CAE Trail that demonstrates that in-service testing (Periodic Testing) will detect degradation before loss of Safety Function.

T13.T02.31 - From the review of the CAE Trail for ESS.4 the following areas for improvement are raised:

- It is not clear where the demonstration is that the initiating variables are 'shown to be sufficient for the purpose of protecting the facility'. Additionally, it appears that the evidence is only related to the Protection System, rather than including other Safety Systems such as SAS. The designer or future operator/licensee is requested to ensure that evidence is identified and included in the CAE Trail that demonstrates that the initiating variables are sufficient for protecting the facility for all Safety Systems.

- In relation to guidance paragraph 339, the interpretations in the argument both appear to miss the point. The 'Limiting Conditions on the Variables' is the limit beyond which an initiating parameter should no go; i.e. if Reactor Trip were to be initiated on high Primary Coolant pressure, then the 'limiting condition' for Primary Coolant pressure (max PC pressure allowed) should not be reached following initiation of Reactor Trip. Hence there should be a suitable margin between initiating value and maximum value to allow for all expected transients. It is not clear that this has been adequately addressed. The designer or future operator/licensee is requested to ensure that the CAE Trail in relation to ESS.4 paragraph 339 is readdressed to demonstrate that Safety Systems respond so that limiting conditions are not transgressed.

T13.T02.32 - From the review of the CAE Trail for ESS.5 the following area for improvement is raised:

- Mention is made of 'Sensor qualification documentation' for provision of response time requirement, but specific reference of these documents is not included in the CAE Trail. The designer or future operator/licensee is requested to ensure that specific reference to supporting evidence documents is included in the CAE Trail.

T13.T02.33 - From the review of the CAE Trail for ESS.6 the following area for improvement is raised:

- It is noted that Primary Coolant Flow is indirectly derived from Main Coolant Pump speed. As this is used in a significant computed variable used for Reactor Trip, there needs to be sufficient justification of the relationship between MCP speed and coolant flow. The designer

Annex 3

or future operator/licensee is requested to ensure that a justification of the relationship between MCP speed and coolant flow is produced and referenced in the CAE Trail.

T13.T02.34 - From the review of the CAE Trail for ESS.17 the following area for improvement is raised:

- The argument does not address whether potential faults (that should be detected by measures to detect failures within safety systems) have been identified that could cause an unsafe change in plant variables (e.g. coolant temperature or pressure rise) if avoidance measures are not initiated. The designer or future operator/licensee is requested to ensure that evidence is identified and cited in the CAE Trail that such faults have been identified.

T13.T02.35 - From the review of the CAE Trail for ESS.25 the following area for improvement is raised:

- The argument for the use of Permissives, Resets and Vetoes is provided against guidance paragraph 358 and applicable evidence documents have been referenced. It would be advantageous if the Argument sections pointed to where this is addressed within the PCSR. The designer or future operator/licensee is requested to ensure that the argument is revised to include reference to appropriate Sections in the PCSR.

T13.T02.36 - From the review of the CAE Trail for ESR.2 the following area for improvement is raised:

- The designer or future operator/licensee is requested to ensure that more specific reference to System Design Manuals (SDMs) and Contract documents is included in the CAE Trail.

T13.T02.37 - From the review of the CAE Trail for ESR.10 the following area for improvement is raised:

- The argument and evidence appear more focused on the control of plant parameters by LCO and Limitation Functions as is discussed more under ESS.9. Whereas this SAP is about failure of control systems, e.g. RCSL, not causing excess demand on safety systems. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to provide sufficient argument and evidence to demonstrate control system failures will not cause excessive demands and evidence of analysis that identifies foreseeable control system faults.

T13.T02.38 - From the review of the CAE Trail for EHF.7 the following area for improvement is raised:

- From a C&I point of view there is no actual argument or evidence relating to the provision of controls, indications, recording equipment and alarms, as required by this SAP. The designer or future operator/licensee is requested to ensure that more specific evidence is identified and cited in the CAE Trail relating to the MCR, RSS, PICS and SICS detailing provisions to meet the requirements of this SAP, not just Human Factors studies related information.

T13.T02.39 - From the review of the CAE Trail for ECS.5 the following area for improvement is raised:

- ECS.5 requires that *'In the absence of applicable or relevant codes and standards, the results of experience, tests, analysis, or a combination thereof, should be applied to demonstrate that the item will perform its safety function(s) to a level commensurate with its classification'*. The only evidence cited is RCC-E that includes the requirements for previous experience, practice, the use of experience feedback for existing components and the use of pre-existing components where standards are not used, but there is no evidence to demonstrate that these requirements have been applied. The designer or future operator/licensee is requested

Annex 3

to ensure that specific evidence of having to adopt results of experience, tests and analysis in the absence of applicable codes and standards is identified and cited in the CAE Trail.

T13.T02.40 - From the review of the CAE Trail for EMT.4 the following areas for improvement are raised:

- The argument put forward for 'no unacceptable degradation of qualification due to maintenance, inspection and testing' all seems to relate to the requirement for EMIT activity with no mention of the requirement to maintain qualification during such activity. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to demonstrate that qualification (e.g. the activities do not stress the system beyond the qualification limits) is maintained during EMIT activities.

- The evidence cited is the 'Requirements for maintenance and test activity'; it is not clear if this stipulates the requirement to maintain qualification or carry out repeat qualification testing following such activity. The designer or future operator/licensee is requested to ensure that the appropriateness of cited evidence is reviewed and specific evidence relating to maintenance of qualification during maintenance activity is included.

T13.T02.41 - From the review of the CAE Trail for EAD.1 the following area for improvement is raised:

- The SAP requires safe working life (SWL) to be defined at the design stage and the 'Claim' states this to be the case. However, the 'argument' discusses the use of maintenance and inspection to detect failures before loss of safety function with no mention of evaluation of SWL (e.g. capacitors, battery backed functions etc.) to define the timescales for EMIT or the replacement date regardless of condition found at EMIT. Guidance paragraphs 194 and 195 are similarly poorly addressed. Additionally, paragraph 195 requires that the SWL exceeds the intended operational life (i.e. time of replacement regardless of condition) by an adequate margin. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to address the evaluation of Safe Working Life at the design stage.

T13.T02.42 - From the review of the CAE Trail for EAD.2 the following area for improvement is raised:

- Guidance paragraph 196 to this SAP is about understanding the effects of material ageing and degradation in the design and making due allowance for it and the rate at which it occurs. The 'arguments' seem to be all about Qualification and EMIT to detect any ageing or degradation. Additionally, the evidence cited is predominantly Site specific processes for EMIT and management of ageing and degradation, whereas evidence that such mechanisms had been taken into account during the design process should be included. The designer or future operator/licensee is requested to ensure that the CAE Trail is revised to address the consideration of material ageing and degradation at the design stage (e.g. insulation materials and tin whiskers etc.).

T13.T02.43 - From the review of the CAE Trail for EES.9 the following area for improvement is raised:

- This SAP is related to the simultaneous loss of both normal and back-up essential services. The RP has stated that, for C&I, essential services are electrical supplies and ventilation. The argument only mentions double power supply without discussion of the simultaneous loss of both. Additionally, there is no reference in the argument or cited evidence to ventilation systems. The designer or future operator/licensee is requested to ensure that the CAE Trail is

Annex 3

revised to address the simultaneous loss of both normal and back-up services, including ventilation systems important to C&I systems and equipment.

T13.T02.44 – Due to unavailability of information from EDF and AREVA, the review of Sensors (In-Core, Ex-Core and Process) was limited to 2 In-Core systems (Self Powered Neutron Detectors (SPND) and Core Outlet Thermocouples (COTs)) against third tier IEC standards using the System Specifications and the RIS System Design Manual. The designer or future operator/licensee is requested to ensure appropriate standards (such as those listed in the BSI NCE 8 list) and processes used in the design, manufacture, procurement, qualification and testing of Sensors are identified and ensure evidence of implementation and compliance to these standards and procedures is produced; this should include evidence of Sensor Qualification for normal and emergency operating conditions.

Conclusions of Task Reviews

With regards to the Adequacy of the PCSR, it is concluded that the general structure of the CAE Approach in response to RO-UKEPR-62 Action A1 demonstrates a sound approach methodology. However, the following need to be addressed in further developing this methodology and its output:

- There needs to be a clear explanation or demonstration of how High Level and Key Claims are derived from appropriate sources, such as C&I Design Requirements Specification, Criteria or Principles, or other appropriate sources.
- There needs to be a clear identification of the location of the Claims and Arguments within the PCSR, and identification of appropriate supporting Evidence.
- The wording of the Claims, particularly the Sub-Claims, appears to be taken directly from the NII SAPs whereas all Claims should be derived independently from the SAPs and relate to the designer's of future operator/licensee's own key claims such as satisfaction of safety principles/criteria. Note: Conformance to HSE C&I SAPs is addressed by RO-UKEPR-62 A.2.

With regards to SAP conformance demonstration, it is concluded that the C&I SAP CAE Trail in document PELL-F DC 9 has developed as an acceptable methodology for the demonstration of conformance to the HSE/ND C&I SAPs. However, there are still significant areas for improvement in the presented Argument and identified Evidence for a large number of SAPs, and most conformance demonstrations for the C&I SAPs have areas for improvement.

With regards to the Sensor review, a sample review of the SPND and COTs System Specifications and the RIS SDM against IEC 61468:2000 and IEC 60737:2010 has shown that some design requirements specified in these IEC standards have been addressed in the System Specification documents and RIS SDM but no clear supporting evidence was identified within them to demonstrate conformance with many areas of the standards. Further detailed evidence is needed as the specific design and procurement progresses.

With regards to the PCSR Updates, it is concluded that:

- The June 2009 Issue 2 of the PCSR did not introduced significant changes to the C&I architecture, nor significant improvements to the safety argumentation presented in the PCSR, compared to the April 2008 Issue 1. The June 2009 Issue 2 of the PCSR had no discernable impact on the preliminary activities conducted under GDA Step 3 Tasks 1 to 3, Task 7 and Task 8.

Annex 3

- The November 2009 Issue 3 of the PCSR C&I sub-chapters and Appendices were sufficiently similar to those in the June 2009 issue to be considered to be identical. As such, the November 2009 Issue 3 of the PCSR had no impact on any GDA Step 3 review work by the TCS Tasks previously undertaken.

In the opinion of the TSC subject to sufficient and adequate responses being made to the TOs/Potential GDA Issues it is anticipated that an adequate position could be confirmed for:

Demonstration of conformance with HSE/ND C&I SAPS.

Demonstration of derivation and identification of a clear CAE Trail for all claims within the UKEPR PCSR.

Confirmation of design, manufacture, test and qualification of Sensors to international standards.

Annex 4

Review of EDF and AREVA QMS Processes Against Principal Design and Implementation Standards – TSC Summary[4]

Note this information has been imported from a TSC report (Ref. 29) and the formatting of the TSC report has been retained.

[4] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 4

A Annex: TSC Task Summary: Review of EDF and AREVA QMS processes against Principal Design and Implementation Standards

This annex summarises the outcome of the Technical Support Contractor's (TSC) review of EDF and AREVA Quality Management System (QMS) processes against principal design and implementation standards and selected Safety Assessment Principles (SAPs) that relate to processes. This review follows on from the review of company-level process-related claims and argumentation carried out in a preliminary activity (Task 4). The aim of the review has been to gain confidence that the Requesting Party (Electricité de France SA and Areva NP SAS, hereafter referred to as EDF and AREVA) have adequate and sufficient evidence to support these process-related claims and arguments. This has included a review of samples of the evidence to support further claims and argumentation presented by EDF and AREVA relating to the conformance of specific C&I systems to selected Safety Assessment Principles (SAPs) that relate to company-level processes.

The task has reviewed C&I company level process-related evidence presented by EDF and AREVA via:

- the claims-argument-evidence table that provides the RP's basis of the demonstration of SAP conformance;
- responses to Technical Queries;
- responses to actions from meetings involving EDF and AREVA, HSE/NII and the TSC;
- and responses to technical observations raised by Task 4, including relevant observations in the HSE/NII Step 2 and 3 reports.

The scope of the task includes company level processes which are applicable to the development of UK EPR Safety and Safety Related C&I equipment. The scope of the evidence that is specific to UK EPR is defined by EDF and AREVA in *"UK EPR CONTROL AND INSTRUMENTATION (C&I) – SCOPE OF GDA"* (letter ND (NII) EPR00686N).

The Pre Construction Safety Report (PCSR) indicates that RCC-E (Design and Construction Rules for Electrical Components of Nuclear Islands, December 2005) defines the process related requirements which are applicable to C&I equipment. This review has therefore sought to confirm that:

- RCC-E addresses the process related requirements of relevant international standards specified by 'BSi Technical Committee NCE/8 Nuclear Power Plants - I&C Systems, A Guide to Applicable IEC standards' (from here on referred to as the 'BSi NCE/8 List');
- RCC-E is encapsulated within the EDF and Areva Quality Management Systems (QMS) and
- RCC-E and the QMS collectively define adequate and sufficient measures for production excellence and independent confidence building.

Regarding standards conformance:

1 Of the IEC standards defined by the BSi NCE/8 List there are 35 standards which are not addressed by RCC-E. However, the standards to be applied on UK EPR will be specified by

Annex 4

reference to RCC-E, plus specific standards identified in technical specifications. With the exception of IEC 61504:2000, EDF and AREVA have committed in response to TQ-EPR-473 to specifying all standards in the BSi NCE/8 List.

2 Based on the sampled evidence, no areas for improvement have been identified with the project-independent processes used by EDF and Areva for the design and implementation of Class 1, 2 and 3 C&I equipment with respect to the requirements of IEC 60880:2006 and IEC 62138:2004.

3 Based on the samples considered in the review, there is adequate and sufficient evidence to demonstrate that project-independent processes used by EDF and Areva for Class 1, 2 and 3 C&I systems satisfy most of the applicable design and implementation, and verification and validation requirements of IEC 61513:2001, IEC 60987:2007 and IEC 61508-2:2000 (where IEC 61508-2:2000 has been the basis of the review for Class 3 hardware.) However there are a number of clauses within the standards for which insufficient evidence has been provided during the period of this review to demonstrate that they are satisfied by project-independent processes.

4 Insufficient evidence has been provided during the period of this review to demonstrate that RCC-E is sufficiently prescriptive in the requirements for the design and implementation of Programmable Complex Electronic Components.

5 Insufficient evidence has been provided during the period of this review to demonstrate that there are adequate company-level processes for the configuration management of the set of all structures, systems and components that comprise the C&I architecture.

6 Based on the sampled evidence, there is adequate and sufficient evidence to demonstrate that RCC-E includes adequate requirements for Independent Verification and Validation and Requirements Management, as required by appropriate IEC standards.

7 Regarding the EDF and Areva Quality Management Systems, based on the sampled evidence there is adequate and sufficient evidence to demonstrate that these systems encapsulate the requirements of RCC-E, and no areas for improvement with the quality assurance arrangements have been identified.

Regarding Independent Confidence Building Measures, the EDF Quality Management System includes processes for quality assessments of system documents, audits and supervision of software development. However, potential GDA Issue pGI-UKEPR-C&I-03.01[5] has been raised for the designer or future operator/licensee to justify the adequacy of independent confidence building activities.

Regarding the demonstration by EDF and AREVA of conformance to SAPs that relate to company-level processes via their claims-argument-evidence submission, no major areas for improvement have been identified. However a number of detailed technical observations (TO) have been raised.

The observations in the HSE/NII report for GDA Steps 2 and 3 have been apportioned to tasks 14 through 18.

The observations in the HSE/NII report for GDA Step 2 which are relevant to this task have been reviewed. Of the 5 that are relevant, 2 are considered by the TSC to be resolved. Some progress has

[5] ND note: GI-UKEPR-CI-02 is the issued version of the provisional GDA Issue (pGI).

Annex 4

been made on the other 3 observations. Outstanding points are covered by the following Technical Observations (TOs) which have been raised in relation to them: T14.TO1.01, T14.TO1.02, T14.TO2.01, T14.TO2.02, T14.TO2.03, T14.TO2.04 and T14.TO2.06. The original Step 2 observations are adequately addressed by these TOs and pGI-UKEPR-C&I-03.01.

None of the observations in the HSE/NII report for GDA Step 3 are relevant to Task 14.

A total of nine technical observations have been raised from this review. These technical observations have been designated TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher. Three of these have been designated TO1, and the other six have been designated TO2.

The TO1 technical observations are:

1 **T14.TO1.01** - The designer or future operator/licensee is requested to ensure that the commitment to apply the standards identified in 'BSi Technical Committee NCE/8 Nuclear Power Plants - I&C Systems, A Guide to Applicable IEC standards' on UK EPR has been fulfilled. EDF and AREVA have stated that this evidence will be in the form of Technical Specifications which will identify standards which complement those identified in RCC-E. The designer or future operator/licensee is also requested to justify why IEC 61504:2000 will not be applied on UK EPR.

2 **T14.TO1.02** - The designer or future operator/licensee is requested to justify the use of programmable complex electronic components (PCECs) in Class 1, 2 and 3 C&I systems. The justification should:

- demonstrate how the requirements of SAPs ECS.3 and ESS.21 paragraph 355 are satisfied and
- identify the standards, guidance and criteria that are used to demonstrate that the components are fit for purpose. In particular the justification should demonstrate that the relevant requirements of IEC 61513:2001 and IEC 60987:2007 have been addressed. (It should be noted that consideration of specific examples of PCECs is addressed as part of Task 15, see S.P1440.74.25 "*Task 15 Class 1&2 System Platforms and Pre-Developed Components Review for UK EPR Reactor*").

3 **T14.TO1.03** - The designer or future operator/licensee is requested to demonstrate that adequate company-level processes, or UK-EPR project-level processes are established for configuration management of the set of all structures, systems and components that comprise the C&I architecture, which should be addressed within an Overall Quality Assurance Plan, or equivalent, as required by IEC 61513:2001 clause 5.4.1.

The TO2 technical observations are:

1 **T14.TO2.01** - The standards identified below are referenced from RCC-E but at an earlier version than that specified by 'BSi Technical Committee NCE/8 Nuclear Power Plants - I&C Systems, A Guide to Applicable IEC standards'.

The designer or future operator/licensee is requested to confirm that the appropriate version of the following standards are specified for UK EPR, or justify the use of earlier versions.

- IEC 60671: 2007

Annex 4

- IEC 60709: 2004
- IEC 61227:2007

2 **T14.T02.02** - There are some clauses within IEC 61513:2001 for which insufficient specific references to sections within RCC-E have been provided to confirm that the requirements of the clause are satisfied.

The designer or future operator/licensee is requested to demonstrate how the following IEC 61513:2001 clauses are addressed within RCC-E or the quality management systems that apply to C&I Safety and Safety Related equipment:

a. Clause 5.1 (Deriving the I&C Requirements from the Plant Safety Design Base)

Insufficient evidence has been found in RCC-E to confirm that the requirements related to the defence in depth concept are satisfied. EDF and AREVA have referred to chapter C6000 of RCC-E, and although it does address issues such as redundancy, independence and reliability, it does not address the principles described in the standard (e.g. prevention from and detection of deviation from normal operation, control of consequences).

b. Clauses 5.2 and 5.5 (Output Documentation):

Chapter C1200 of RCC-E describes at a high level the type of documents to be produced. However, there is insufficient detail to confirm that the requirements of clauses 5.2 and 5.5 are satisfied.

It is also noted that chapter C5231 defines some documentation requirements. However, these only apply to Class 1 and 2 systems, not Class 3.

c. Clauses 5.4.3 and 7 (Overall Integration and Commissioning)

No requirements have been found within RCC-E for an Overall Integration and Commissioning Plan.

d. Clause 5.4.4 and 8 (Operation Plan)

No requirements have been found in RCC-E for an Overall Operation Plan.

3 **T14.T02.03** - There are some clauses within IEC 60987:2007 for which insufficient specific references to sections within RCC-E have been provided to confirm that the requirements of the clause are satisfied.

The designer or future operator/licensee is requested to demonstrate that the following IEC 60987:2007 clauses are addressed within RCC-E or the quality management systems that apply to C&I Safety and Safety Related equipment:

a. Clause 5.2 (Functional and Performance Requirements)

Chapter C5200 of RCC-E identifies the need for a Hardware Specification, however it states that this is outside the scope of this chapter, and does not indicate where it is addressed.

Annex 4

b. Clause 5.5 (Documentation Requirements)

Chapter C1200 of RCC-E describes at a high level the type of documents to be produced. However, there is insufficient detail to confirm that the requirements of clause 5.5 are satisfied.

c. Clauses 6.1, 6.2 (Design Activities)

Chapter C5000 of RCC-E "*Development of Programmable Systems*" provides requirements for the design and production of programmable systems (e.g. definition of requirements, production of architectural documents). However, it does not describe the development lifecycle for hardware components.

d. Clause 6.7 (Power Failure)

No evidence has been found in RCC-E to demonstrate that clause 6.7 is satisfied.

e. Clause 9 (Manufacture)

Chapters A3300 and B1000 of RCC-E provide some information on the procurement for components. However, there is no indication that they are assessed against the requirements of IEC 60987.

f. Clause 11 (Maintenance)

Chapter C3400 of RCC-E provides some information on Maintenance. However, no requirements have been found in RCC-E for the recording of failure data, or maintenance records.

4 **T14.T02.04** - There are some clauses within IEC 61508-2:2000, which apply to Electrical/Electronic/Programmable Electronic Systems (E/E/PS), for which insufficient specific references to sections within RCC-E have been provided to confirm that the requirements of the clause are satisfied (where IEC 61508-2:2000 has been the basis of the review of the processes for Class 3 hardware.)

The designer or future operator/licensee is requested to demonstrate that the following IEC 61508-2:2000 clauses are addressed within RCC-E or the quality management systems that apply to C&I Safety and Safety Related equipment:

a. Clause 7.4 (design and development)

Chapter C5000 provides information on the development of programmable systems (e.g. definition of requirements, production of architectural documents).

However, it does not describe a development lifecycle for hardware components.

b. Clause 7.4 (E/E/PES design and development)

Annex 4

Chapter C5200 identifies the need for a Hardware Specification, and Architecture Definition. However it states that these are outside the scope of this chapter, and does not indicate where they are addressed.

c. Clause 7.4 (E/E/PES design and development)

There is insufficient evidence to confirm that RCC-E satisfies the detailed hardware related requirements of clauses 7.4.3, 7.4.7 and 7.4.8.

d. Clause 7.6 (E/E/PS/Operation and Maintenance Procedures)

Chapter C3400 provides some information on Maintenance. However, no requirements have been found in RCC-E for the recording of failure data, or maintenance records.

e. Annexes A, B, C

Insufficient evidence has been found in RCC-E to confirm that RCC-E satisfies the detailed hardware related requirements of Annexes A, B and C.

5 **T14.T02.05** - The designer or future operator/licensee is requested to address the following observation which has arisen from the review of the Claims-Argument-Evidence (CAE) for Safety Assessment Principle (SAP) EQU.1 (Equipment Qualification).

Chapter B3500 of RCC-E states that qualification shall be in accordance with IEC 60780:1998 clause 5.3. However, it does not indicate which chapters within RCC-E address other clauses in IEC 60780:1998.

The designer or future operator/licensee is requested to update the CAE to demonstrate that the requirements of IEC 60780:1998 are satisfied within RCC-E or the quality management systems that apply to C&I,

6 **T14.T02.06** - The designer or future operator/licensee is requested to address the following observations which have arisen from the review of the CAE for SAP ESS.27 (Safety Systems - Computer-based safety systems).

a. The CAE refers to NLF-F DC 369, "Qualification of SPPA T2000 Systems". The purpose of the document in the context of the argument is not explained.

The designer or future operator/licensee is requested to update the CAE to explain the purpose of NLF-F DC 369 in the context of the argument.

b. There is no evidence referenced from the claim and argument for processes for independent assessment of the test programme, covering the full scope of test activities.

The designer or future operator/licensee is requested to update the CAE to demonstrate that the requirements for independent assessment of the test programme are satisfied.

Conclusion of Task Review

Annex 4

In the opinion of the TSC, based on the sampled evidence, and subject to satisfactory resolution of the technical observations, no evidence was found to indicate that the claims and argument made for the inclusion of requirements for standards conformance within company-level processes are not supported. There is insufficient evidence to demonstrate that company-level processes define an adequate set of independent confidence building measures such as independent testing and software static analysis.

Annex 5

Review of Class 1 and 2 System Platforms and Pre-Developed Components C&I – TSC Summary[6]

Note this information has been imported from a TSC report (Ref. 30) and the formatting of the TSC report has been retained.

[6] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 5

A Annex: TSC Task Summary: Review of Class 1&2 System Platforms and Pre-Developed Complex Components

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of Class 1&2 System Platforms and Pre-Developed Complex Components (TSC Task 15) for the UK EPR reactor design.

This review follows on from the review of Pre-Developed Class 1 System Platforms carried out in a preliminary activity (TSC Task 5).

The aim of the review has been:

- To determine the adequacy and sufficiency of the evidence provided by the Requesting Party (EDF Energy and Areva NP, hereafter referred to as EDF and AREVA) to support claims and arguments of the application of appropriate standards and guidance to the production of the platform.

  This has included review of the evidence to support further claims and argumentation presented by EDF and AREVA relating to the conformance of specific Control & Instrumentation platforms to selected Safety Assessment Principles (SAPs). The SAPs considered relate to necessary characteristics of such platforms to fulfil C&I requirements. Eleven SAPs have been considered in the timescales of the review (EQU.1 - Qualification procedures, EDR.1 - Failure to safety, EDR.2 - Redundancy, diversity and segregation, EDR.3 - Common cause failure, ESS.1 - Requirement for safety systems, ESS.21 - Reliability, ESS.23 - Allowance for unavailability of equipment , ESS.27 - Computer based safety systems, ESR.3 - Provision of controls, ESR.5 - Standards for computer based equipment, ESS.15 - Alteration of configuration, operational logic or associated data).

- To determine from the evidence provided by the Requesting Party that the functionality and performance of the TELEPERM XS platform are adequate and sufficient for deployment in a Class 1 system through a focused review of:
  - Deterministic behaviour of the TELEPERM XS platform by considering:
    - Avoidance of internal and external interference;
    - Avoidance of concurrent interactions including asynchronous interrupts;
    - Predictability of execution and communication;
    - Fully defined states and modes of operation;
    - Static Memory Management.
  - Self Checking and Fault Management of the TELEPERM XS platform by considering:
    - Existence and definition of Memory Tests;
    - Existence and definition Processor Instruction Tests;

Annex 5

- Detection of random hardware failures and subsequent action;
- Detection of erroneous software behaviour and subsequent action;
- Detection of data transmission corruption/errors and subsequent action;
- Detection of discovery program over run and subsequent action;
- Determination of validity of inputs.

- Gain confidence that the Requesting Party has adequate evidence to support claims and arguments of the application of appropriate standards and guidance to the production of the Non Computerised Safety System;
- Gain confidence that the methodology used for the qualification of the Smart devices used in nuclear safety function is adequate.

The task has reviewed samples of platform-related evidence presented by EDF and AREVA via:

- the claims-argument-evidence table that provides the RP's basis of the demonstration of SAP conformance;
- responses to Technical Queries;
- responses to actions from meetings involving EDF and AREVA, HSE/NII and the TSC; and
- responses to technical observations raised by the preliminary activity known as Task 5, including platform-related observations in the HSE/NII Step 2 and 3 reports.

The C&I architecture has been modified significantly since the definition that was presented by EDF and AREVA in Step 3 in response to Regulatory Issue RI-UKEPR-02. The proposed addition of the Non-Computerised Safety System has resulted in reduced reliability claims for the primary (TELEPERM XS) and secondary (SPPA_T2000) protection systems ($1E^{-4}$ pfd and $1E^{-2}$ pfd respectively) which has been recorded in Section 2 of the attachment to EDF and AREVA letter EPR00180R. The scope of the Step 4 Task 15 review therefore covers the Teleperm XS (including the Qualified Display System) version 3.5.3, SPPA-T2000 version S5 and Non Computerised Safety System (NCSS) platforms. The scope of the review also covers Smart devices as pre-developed components.

A total of 57 detailed observations resulting from the review have been raised. These technical observations have been designated TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher – 11 of these observations have been designated TO1 and 46 of these observations have been designated TO2.

By analysing the detailed observations a set of high level areas for improvement was recognised. The following sections provide details on the technical observations raised during the review.

Some Technical Observations raised during the review were subsumed by other Technical Observations or resolved before this report was issued. These Technical Observations are:

- T15.TO2.04 has been subsumed by T15.TO2.02;

Annex 5

- **T15.TO2.20, 21 & 23 have been subsumed by T15.TO2.19; and**
- **T15.TO2.56 has been resolved as a further review of the sampled evidence which was applicable to SAP EDR.2 addressed the technical observation.**

Annex 5

T15.TO2.01 - Response to Task 5 Report Observations

The TSC report *Task 5 Pre-Developed Class 1 System Platforms Review for UK EPR Reactor S.P1440.54.15, Issue 1.4* identified 38 Technical Observations which were also recorded in Technical Query TQ-EPR-571. EDF and AREVA has not provided a formal response to this TQ within the timescales of this review.

The TSC has performed a review of the 38 Technical observations and it is the opinion of the TSC that 9 of these observations have not been addressed through evidence seen during the Task 15 review.

a) **EPR.T5.7 - The *ISTec report ISTec Assessment of application of tools for TELEPERM XS, ISTec - A – 1085. Rev. 0, June 2006* documents the ISTec assessment of the tools that are part of the TELEPERM XS platform. This has led to a number of points for which the designer or future operator/licensee is requested to address:**

   i. **Some tools were not assessed by ISTec in detail (e.g. code generators) because they were type-tested by GRS. However clauses 13 and 14.2 of IEC 60880:2006 require that the defence in depth principles should be considered in the development, selection and use of tools. For these tools the only protection provided against failures is their type testing.**

      The designer or future operator/licensee is requested to justify that the qualification of these tools is adequate, and why other protections (e.g. validation of their outputs) are not considered.

   ii. **The argument for the adequacy of the SPACE editor is that its output can be verified by another tool, and that it has a considerable amount of operational experience. While this could be an acceptable argument, it is only valid if it can be assured that the output is verified.**

      The designer or future operator/licensee is requested to demonstrate how the output from the SPACE editor is verified when it is used in the development of specific applications as required by IEC 60880:2006, clause 14.2 (limits of applicability of tools).

   iii. **Some tools were developed in accordance with internal assurance procedures. The designer or future operator/licensee is requested to justify that the internal assurance procedures meet the requirements of IEC 60880.**

   iv. **For several tools (e.g. hwparams, swparams), it is stated that they are only used for documentation purposes, and hence do not have a safety impact. The designer or future operator/licensee is requested to justify how documentation generated by such tools has no safety impact as required by IEC 60880, clause 14.2 (limits of applicability of tools).**

   v. **For some tools, it is stated that they are not suitable, or have restricted use, for verification tasks. (e.g. cpuload, netload, rediff). The designer or future operator/licensee is requested to demonstrate that tools stated as not suitable for, or have restricted use for verification tasks, are not used for such purposes as required by IEC 60880, clause 14.2 (limits of applicability of tools).**

b) **EPR.T5.8 - Section 6 of the *United States Nuclear Regulatory Commission Safety Evaluation by the Office of Nuclear Reactor Regulation Siemens Power Corporation Topical Report EMF-2110 (NP), "Teleperm XS: A digital Reactor Protection System" Project No. 702. Dated 5th May 2000* report identifies a number of conditions that need to be satisfied when using the TELEPERM XS in specific applications.**

Annex 5

The designer or future operator/licensee is requested demonstrate that the 17 actions recorded in *Section 6.0 Plant-Specific Items* of the report *United States Nuclear Regulatory Commission Safety Evaluation by the Office of Nuclear Reactor Regulation Siemens Power Corporation Topical Report EMF-2110 (NP), "Teleperm XS: A digital Reactor Protection System" Project No. 702. Dated 5th May 2000* have been addressed for the UK EPR.

c) EPR.T5.11 - The information available to the reviewer does not describe the relationship between the safety and software lifecycles. Also, there is no description of organisational team structure and roles with respect to approvals and independence.

The designer or future operator/licensee is requested to:

1. Demonstrate that processes are in place to manage the interface and interactions of the safety and software lifecycles, and that these processes have been adhered to; and

2. Justify that the processes meet the requirements of clause 5.4 of IEC 60880, and clause 6 of IEC 61513.

d) EPR.T5.18 - Section 3.2.2 *"Integration and System Test"* of *"TELEPERM XS: A digital Reactor Protection system EMF-2110 (NP)(A) Revision 1" states the* following:

> *"The test was done using the test field with the original hardware and software of the first large TELEPERM XS application. This application was the limitation and control system for the Nuclear Power Plant in Untersweser".*

The designer or future operator/licensee is requested to justify that the testing evidence gained using the test field based on the limitation and control system for the Nuclear Power Plant in Untersweser is applicable when its use is claimed for the UK EPR.

e) EPR.T5.21 - There is insufficient information to demonstrate that requirements of clause 14 of IEC 60880 have been satisfied for qualification of the compiler as the qualification evidence only cites service history. The designer or future operator/licensee is requested to demonstrate that the compilers used for the TELEPERM XS platform are suitable for the development of Class 1 systems.

f) EPR.T5.26 - The designer or future operator/licensee is requested to demonstrate that conformance with the standard KTA 3503 satisfies the requirements of IEC 60987 for manufacturing.

g) EPR.T5.28 - With regard to the Common Position of Seven European Nuclear Regulators and Authorised Support Organisations, Revision 2007, chapter 1.1 (Safety Demonstration), there is no clear evidence provided to indicate that a Safety Plan for TELEPERM XS was produced to address topics such as:

- organisational arrangements;
- demonstration that system/software/hardware requirements satisfy safety requirements;
- independence of those undertaking the safety demonstration activities; and
- safety demonstration strategy

Annex 5

The designer or future operator/licensee is requested to demonstrate that the requirements of this chapter have been satisfied.

h) **EPR.T5.31 - With regard to the Common Position of Seven European Nuclear Regulators and Authorised Support Organisations, Revision 2007, chapter 1.5 (Tools).**

The designer or future operator/licensee is requested to demonstrate that faults cannot be introduced/not detected by the TELEPERM XS development and verification tools, or that adequate measures are established to detect the introduction of potential tool-introduced faults.

i) **EPR.T5.34 - The information given in the TELEPERM XS documentation *TELEPERM XS: A Digital Reactor Protection System, EMF-2110 (NP)(A), Revision 1* does not present evidence in accordance with the requirements of clause 6 "System Safety Life Cycle" (and its sub-clauses) of IEC 61513:2001.**

The designer or future operator/licensee is requested to demonstrate how the TELEPERM XS satisfies requirements of clause 6 "System Safety Life Cycle" (and its sub-clauses) of IEC 61513.

T15.TO1.02 - TELEPERM XS Platform - Justification for the use of Programmable Complex Electronic Components in Class 1 C&I Systems

a) **The designer or future operator/licensee is requested to justify the use of programmable complex electronic components in the TELEPERM XS components that are part of Class 1 C&I systems. The justification should identify the standards, guidance and criteria that are used to demonstrate that the components are fit for purpose, and the evidence of their application. Note: a provisional development standard for programmable complex electronic components and a process for its application has been identified in EDF and AREVA letter *Response to TATS action 36-I&C5 Explanation of the Basis for the Qualification of the CEC - EPR00741N.***

b) **The designer or future operator/licensee is requested to complete a Programmable Complex Electronic Component Checklist S.P1440.074.013 Issue 2.2.2 for the TELEPERM XS SVE2 and ESCC2 components.**

T15.TO1.03 - TELEPERM XS Platform – Scope of Application of Programmable Complex Electronic Components/Configware Campaign

The review activity addressed EDF and AREVA's explanation of the basis of Qualification of Programmable Complex Electronic Components. A review of EDF and AREVA letter *Response to TATS action 36-I&C5 Explanation of the Basis for the Qualification of the CEC - EPR00741N* was performed.

The designer or future operator/licensee is requested to ensure that the Complex Electronic Components/Configware campaign stated in EDF and AREVA letter *Response to TATS action 36-I&C5 Explanation of the Basis for the Qualification of the CEC - EPR00741N* is applied for all TELEPERM XS modules that contain such components that are being used on UK-EPR.

TELEPERM XS Platform - General Process Areas for Improvement

The review of the TELEPERM XS Platform against International Nuclear Standards highlighted several areas for improvement that the designer or future operator/licensee is requested to address.

Annex 5

T15.TO2.05 - A TELEPERM XS IEC 60987 conformance matrix has not been made available within the timescales of the review. The designer or future operator/licensee is requested to demonstrate conformance with IEC 60987. This demonstration is to cover all TELEPERM XS hardware components that will be used on the UK EPR.

T15.TO2.06 – The Teleperm XS IEC 60880 conformance matrix for TELEPERM XS platform software has not been made available within the time scales of this review. The designer or future operator/licensee is requested to demonstrate conformance with IEC 60880.

T15.TO2.07 - The scope of static analysis to be applied to the TELEPERM XS platform software has not been defined within the timescales of this review. The designer or future operator/licensee is requested to define fully the level of static analysis to be applied to the TELEPERM XS platform software components used for the UK EPR.

T15.TO2.08 – Section 2 of the *Software Tests, TXS-4.1en, Revision A* states the following for module tests:

> *'A white-box test of a piece of software, usually performed by the implementer as a smoke test (quick test of basic functionality) and/or verification of software at the deepest level (normally inside the software development environment)'.*

From this it is understood that software development involves informal testing and debugging. However, clause 8.2.3.1 of IEC 60880:2006 requires module testing to be a formal verification activity and *Software Tests, TXS-4.1en, Revision A* suggests a degree of informality, with a lack of specific test criteria to be satisfied at this level. A Technical Query was raised concerning this but no response was received during the timescales of this review. The designer or future operator/licensee is requested to ensure evidence is produced that demonstrates that clause 8.2.3.1 of IEC 60880 is satisfied for module testing.

T15.TO2.09 - No conformance statement for TELEPERM XS platform development against the requirements of IEC 61513 has been provided in the timescales of this review. The designer or future operator/licensee is requested to demonstrate conformance with IEC 61513 for the TELEPERM XS platform development.

T15.TO2.10 - Insufficient information on the TELEPERM XS software platform aspects of installation and operation has been provided in the timescales of this review. There is an expectation from IEC 60880 clause 12 for an Installation/Commissioning Plan/Procedure to be in place for installing and commissioning a given release of the software for initial and/or modification purposes. The Installation/Commissioning Plan/Procedure should address:

1. Security processes (including any bypasses required for installation);
2. Verification processes (to check the validity/integrity of the installed software).

The designer or future operator/licensee is requested to ensure evidence on the Installation and Operational aspects of the TELEPERM XS software platform is produced in conformance with IEC 60880 clause 12.

Annex 5

T15.TO2.11 - TELEPERM XS Platform – Software Tools

The review of the TELEPERM XS platform included a review of tools used to develop the platform software and tools developed to support the production of TELEPERM XS based applications.

Insufficient information has been provided in the timescale of the review on the TELEPERM XS software development process for new software tool selection and strategy for tool upgrade and replacement.

The designer or future operator/licensee is requested to ensure evidence of process for new software tool selection and strategy for tool upgrade and replacement is available.

TELEPERM XS Platform - Requirements Management, Traceability and Document Hierarchy

The review of the TELEPERM XS platform identified several technical observations with respect to Requirements Management, Requirements Traceability and Documentation Hierarchy.

EDF and AREVA presented a current process improvement programme which addresses Requirements Management, Requirements Traceability and Documentation Hierarchy.

T15.TO2.12 - TELEPERM XS safety requirements should be explicitly identified and provide clear traceability to the tests and test results that demonstrate that they have been met. The designer or future operator/licensee is requested to ensure a process is implemented on the UK-EPR which manages safety requirements and their traceability to test case/procedure and test results. The designer or future operator/licensee is also requested to demonstrate adequacy of the process.

T15.TO2.13 - A TELEPERM XS Platform requirement specification should be produced from which hardware and software requirements can be derived. The designer or future operator/licensee is requested to ensure a process is implemented on the UK-EPR that identifies the production of a Requirements Specification from which hardware and software requirements can be derived. The designer or future operator/licensee is also requested to demonstrate adequacy of the process.

T15.TO2.14 - There is area for improvement in the traceability from TELEPERM XS Platform requirements to test case/procedure to test results. The designer or future operator/licensee is requested to ensure a process is implemented on the UK-EPR to manage requirements and their traceability to test case/procedure and test results. The designer or future operator/licensee is also requested to demonstrate adequacy of the process.

T15.TO2.15 - There should be clear traceability from requirements into all levels of test, specifically to TELEPERM XS Platform Integration Tests. The designer or future operator/licensee is requested to ensure a process is implemented on the UK-EPR to manage requirements and their traceability to TELEPERM XS Platform Integration test case/procedure and test results. The designer or future operator/licensee is also requested to demonstrate adequacy of the process.

T15.TO2.16 - All documents used as inputs to platform test activities should be clearly identified within the documentation hierarchy and also in the applicable quality plans. The designer or future operator/licensee is requested to ensure a process is implemented on the UK-EPR to manage requirements and a definition of the documentation hierarchy that demonstrate requirements traceability through the Teleperm XS lifecycle data. The designer or future operator/licensee is also requested to demonstrate adequacy of the process.

Annex 5

T15.TO2.17 - TELEPERM XS Platform - Use of Formal Methods to Identify Failure Modes

IEC 60987:2007 clause 5.3 has an expectation that Mean Time Between Failure for revealed and un-revealed failures are specified as system platform requirements. The reviewed TELEPERM XS components user manuals *(Teleperm XS User Manual SPAM1 Programmable analogue signal processing module (6FK5327-8AA00) TXS-2601-76-V1.1 and Teleperm XS User Manual SVE2 processing module (6FK5206-8AA/-8AE/-8BA/-8BE) TXS-1020-76-V3.0)* present Failure In Time and make a claim that the Failure In Time values are based on comparable components.

The designer or future operator/licensee is requested to:

- **Justify how Failure In Time relates to Mean Time Between Failure for revealed and un-revealed failures;**
- **Justify how Failure In Time values can be based on Failure In Time values of comparable products.**

T15.TO1.18 - TELEPERM XS Platform - Role of the External Independent Assessor in Software Production Excellence and Independence Confidence Building Measures

EDF document *RI-UKEPR-002 Answer to Action A1.5 – Production Excellence and Independent Confidence Building for EPR UK safety I&C, ENSECC090137 Revision B* section 3.1 identifies that the external independent assessment of the TELEPERM XS platform software is part of their Independent Confidence Building Measures. However during the review meetings on 3, 4 & 5 Aug and 30th Sept 2010 it was indicated that parts of the External Independent Assessor's activities were being used as part of the platform software Production Excellence argument, specifically:

- **Managerial Independence of Verification activity (IEC 60880 clause 8.1.2);**
- **Independence of Developers and Verifiers (IEC 60880 clause 8.1.1);**
- **The timing of the independent verification activities within the overall software development lifecycle (production excellence) as presented in Figure 3 of IEC 60880 (IEC 60880 clause 8.1.12 & 8.1.13).**

The designer or future operator/licensee is requested to:

1. **Clearly identify the role of the External Independent Assessor as being part of Software Production Excellence or Software Independent Confidence Building Measures (it cannot meet the needs of both);**
2. **If the role of the External Independent Assessor is identified as part of the Software Independent Confidence Building Measures then the designer or future operator/licensee is requested to:**
    a. **Identify compensating measures to fulfil the requirements of IEC 60880 clauses 8.1.1, 8.1.2, 8.1.12 & 8.1.13;**
    b. **Investigate the reasonable practicality of enhancing the current software verification process for new and modified software so that it meets the requirements of IEC 60880 clauses**

Annex 5

8.1.1, 8.1.2, 8.1.12 & 8.1.13 or provide justification that the existing arrangements meet the requirements of IEC 60880 clauses 8.1.1, 8.1.2, 8.1.12 & 8.1.13.

T15.TO1.19 - TELEPERM XS Platform - Role of the External Independent Assessor in Hardware Development and Verification Activities

EDF document *RI-UKEPR-002 Answer to Action A1.5 – Production Excellence and Independent Confidence Building for EPR UK safety I&C, ENSECC090137 Revision B* section 3.1 identifies that the external independent assessment of the TELEPERM XS platform hardware is part of their Independent Confidence Building Measures. However during the review meetings on 3, 4 & 5 Aug and 30th Sept 2010 it was indicated that parts of the External Independent Assessor's activities were being used as part of the platform hardware development and verification argument, specifically:

- **Independence of Verification activity (IEC 60987 clause 7.3.1);**
- **Timing of verification activities (IEC 60987 clause 7.1.1).**

The designer or future operator/licensee is requested to:

1 **Clearly identify the role of the External Independent Assessor as being part of hardware development and verification or hardware independent assessment (it cannot meet the needs of both);**

2 **If the role of the External Independent Assessor is identified as part of the hardware independent assessment then the designer or future operator/licensee is requested to:**

   a **Identify compensating measures to fulfil the requirements of IEC 60987 clauses 7.1.1 & 7.3.1;**

   b **Investigate the reasonable practicality of enhancing the current hardware verification process for new and modified software so that it meets the requirements of IEC 60987 clauses 7.1.1 & 7.3.1.**

TELEPERM XS Platform - Software Module and Integration Test Independence

T15.TO2.22 - TELEPERM XS platform Software Module and Integration Test independence does not meet the objectives of IEC 60880 clause 8.1.2 i.e. they may be in the same team, therefore not managerially independent. The designer or future operator/licensee is requested to justify that the current arrangements for the Software Production Excellence Verification and Validation activities meet the requirements of IEC 60880 clause 8.1.2. If this is not achievable the designer or future operator/licensee is requested to identify appropriate compensating measures.

TELEPERM XS Platform - Systematic Formal Checks of Hardware Lifecycle Data Items

T15.TO2.24 - Areva documents *Summary Qualification Report for SVE2 - 8BA/BE and SBU1/SKO1 - 8BA, NLTCG/2007/en/0039, Rev C, TXS-PrÜfspezifikation: TypprÜfung der FUTIS I/O Komponenten SAI, SAO, SDI, SDO, SGPIO. NGLTD/2005/de/0230 Rev A,* and *Documentation of theoretical and practical testing according to KTA 3503 of the Overvoltage barrier modules SOBx-y, ID-No's 6FK5325-8AA01 ... -8AA05 from the system TELEPERM XS of the company AREVA NP GmbH, TÜV Rheinland, 968/K 138.00/06* identify the hardware lifecycle documents subject to theoretical test by Technischer

Annex 5

Überwachungsverein, and a general statement is made in these reports about whether each document is as expected or not. The documents identified are consistent to those required by *Safety Standards of the Nuclear Safety Standards Commission (KTA) - Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System - KTA 3503 (11/2005)* however it is not possible to determine if all lifecycle data has been subject to systematic formal checks. The designer or future operator/licensee is requested to ensure systematic formal checks have been applied to all hardware lifecycle data items. If this is not achievable the designer or future operator/licensee is requested to identify appropriate compensating measures.

TELEPERM XS Platform – Review Approach and Criteria of the Independent Assessor

T15.TO2.25 - The Technischer Überwachungsverein test type reports for TELEPERM XS components indicate that reviews were performed but no details on how reviews were conducted and the criteria used for review are identified. The designer or future operator/licensee is requested to justify and make available details of Technischer Überwachungsverein's review approach and criteria.

TELEPERM XS Platform - Claims Made Against the Use of KTA3503

During the review Hardware Qualification was addressed. TELEPERM XS Platform hardware components are qualified against German Nuclear standard *Safety Standards of the Nuclear Safety Standards Commission (KTA) - Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System - KTA 3503 (11/2005),* however it was noted that inappropriate claims were being made against the standard with respect to its scope and its application of IEC 60780.

T15.TO2.26 - *Safety Standards of the Nuclear Safety Standards Commission (KTA) - Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System - KTA 3503 (11/2005)* only refers to IEC 60780 as informative and does not directly respond to it, so no claim can be made that IEC 60780 has been applied. The designer or future operator/licensee is requested not to quote *Safety Standards of the Nuclear Safety Standards Commission (KTA) - Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System - KTA 3503 (11/2005)* in response to making claims against IEC 60780 unless this is appropriately justified.

T15.TO2.27 - *Safety Standards of the Nuclear Safety Standards Commission (KTA) - Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System - KTA 3503 (11/2005)* is a standard for performing Type Testing and is not a standard covering the full development lifecycle, so no claim against Areva's full hardware development lifecycle can be made by citing *Safety Standards of the Nuclear Safety Standards Commission (KTA) - Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System - KTA 3503 (11/2005)*. The designer or future operator/licensee is requested not to quote *Safety Standards of the Nuclear Safety Standards Commission (KTA) - Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System - KTA 3503 (11/2005)* in response to claims made against the full development lifecycle of the TELEPERM XS unless this is appropriately justified.

TELEPERM XS Platform - Qualification

During the review Hardware Qualification of the TELEPERM XS was addressed and several technical observations were made.

Annex 5

T15.TO2.28 - Review of EDF and AREVA documents *Compliance of the TXS Hardware Design and Engineering Process with IEC60987 Ed 2 NLTC-G/2008/en/0053, Revision A* and *Overview of approach for TXS hardware qualification NLTC-G/2007/en/0072, Revision A* provided no information how Qualified Target Life (as identified in IEC 60987 clause 6.2.5) is addressed for the TELEPERM XS platform hardware. The designer or future operator/licensee is requested to demonstrate that their hardware qualification process addresses Qualified Life.

T15.TO2.29 - From the evidence sampled no evidence could be found that specified the Qualified Life (as required by IEC 60780 Section 4) for the TELEPERM XS platform hardware. The designer or future operator/licensee is requested to demonstrate that the hardware qualification process addresses Qualified Life.

T15.TO2.30 - EDF and AREVA use a standard approach to equipment qualification that is presented in document *Teleperm XS General Specification for Equipment Qualification of I&C Components of Class 1E for mild environment NLTD-G/2008/en/0229 Rev C*. A review of Summary Qualification Reports provided for components SVE2, SOB and SDIx (*Summary Qualification Report for SVE2 - 8BA/BE and SBU1/SKO1 -8BA, NLTCG/2007/en/0039 Rev C, Summary Qualification Report: Qualification of the Overvoltage Barrier Modules SOB1-24, SOB1-48, SOB2-24, SOB2-48, SOB3 and SOB31-24. NLTC-G/2007/en/0014, Rev A and Summary Qualification Report for the binary input modules SDI1-24, SDI2-24, SDI1-48 and binary output modules SDO1-24, SDO1-48, NLTC-G/2007/en/0028, Rev B respectively*) could not determine if this standard approach has been applied. For UK-EPR the designer or future operator/licensee is requested to justify that an adequate qualification process has been applied to the applicable TELEPERM XS components.

T15.TO2.31 - The standard approach to equipment qualification that is presented in document *Teleperm XS General Specification for Equipment Qualification of I&C Components of Class 1E for mild environment NLTD-G/2008/en/0229 Rev C* provides no guidance on Pre-Ageing as identified in IEC 60780 Clause 5.3.3. The designer or future operator/licensee is requested to ensure the hardware qualification process addresses Pre-Ageing.

T15.TO2.32 - The Summary Qualification Reports provided for SVE2, SOB and SDIx (*Summary Qualification Report for SVE2 - 8BA/BE and SBU1/SKO1 -8BA, NLTCG/2007/en/0039 Rev C, Summary Qualification Report: Qualification of the Overvoltage Barrier Modules SOB1-24, SOB1-48, SOB2-24, SOB2-48, SOB3 and SOB31-24. NLTC-G/2007/en/0014, Rev A and Summary Qualification Report for the binary input modules SDI1-24, SDI2-24, SDI1-48 and binary output modules SDO1-24, SDO1-48, NLTC-G/2007/en/0028, Rev B respectively*) do not appear to identify if pre-ageing as identified in IEC 60780 Clause 5.3.3 has been addressed or justification provided as to why pre-aging is not appropriate. The designer or future operator/licensee is requested to demonstrate that Pre-Aging has been applied prior to the qualification of parts of the TELEPERM XS platform where it is appropriate.

TELEPERM XS Platform - Frequency of Reporting of Self Test Results

As part of the review activity a deep sampling of evidence specific to TELEPERM XS Platform self test was performed and several technical observations relating to self test were made.

T15.TO2.33 - The designer or future operator/licensee is requested to demonstrate that the frequency of the TELEPERM XS memory checks are performed at a sufficient rate to detect and report memory failures in a timely manner.

Annex 5

T15.TO2.34 - The designer or future operator/licensee is requested to demonstrate that for TELEPERM XS on a cycle overrun, the fault condition is communicated in a manner that allows appropriate corrective/mitigating actions to be performed.

T15.TO2.35 - The designer or future operator/licensee is requested to demonstrate that for TELEPERM XS on failure to complete self test, the fault condition is communicated in a manner that allows appropriate corrective/mitigating actions to be performed.

T15.TO2.36 - TELEPERM XS Platform – Estimation of Processor Utilisation

As part of the review, determining the processor utilisation of TELEPERM XS platform software was considered. Although evidence exists to demonstrate that processor utilisation of the TELEPERM XS platform software has been measured using specialist TELEPERM XS platform tools, no evidence had been provided reporting the timescales of this review to demonstrate that worst case timing scenarios had been used.

For TELEPERM XS the designer or future operator/licensee is requested to demonstrate that worst case timing scenarios have been used when determining processor utilisation of the TELEPERM XS platform software.

T15.TO2.37 - TELEPERM XS Platform – Fault and Change Management

During the review activity, the Fault and Change Management System applied to the TELEPERM XS Platform was reviewed. The TELEPERM XS Platform Fault/Change Management activities are controlled using the open source tool "Request Tracker" that enforces a Fault/Change Management Lifecycle and its use and application appears appropriate. However there is no detailed documented approach to Fault/Change Management which will allow each phase of the Fault/Change Management Lifecycle to be performed in a consistent and repeatable way.

The designer or future operator/licensee is requested to ensure a detailed TELEPERM XS Platform Fault/Change Management process that can be applied consistently and in a repeatable way is implemented, and which should also include a systematic approach to impact analysis and regression testing.

T15.TO1.38 - SPPA T2000 Platform – Adequacy of Testing and Test Evidence

EDF and AREVA have indicated (in response to Technical Query TQ-EPR-1133) that EDF, Areva and Siemens are issuing a report describing the strategy, principles and coverage of the tests performed for AS620B Automation System and particularly for the System Software due to concerns raised by Autorité Sûreté Nucléaire (French Nuclear Safety Authority).

The designer or future operator/licensee is requested ensure the areas for improvement identified in the report are addressed and ensure the requirements for production excellence of a Class 2 system (at the integrity level used for the UK-EPR) have been met.

T15.TO1.39 - SPPA T2000 Platform - Evidence on the Application of IEC 60987

Evidence on the application of IEC 60987 (including IEC 60780) to SPPA-T2000 hardware development has not been provided within the timescales of this review. The designer or future

Annex 5

operator/licensee is requested to demonstrate conformance with IEC 60987 (including IEC 60780) for SPPA-T2000 hardware development for existing hardware and any newly developed hardware.

SPPA T2000 Platform - Production Excellence

The sample based review of the SPPA T2000 platform identified several areas for improvement on production excellence:

T15.TO2.40 - SPPA-T2000 hardware development process or lifecycle data was not provided in the timescales of this review. The designer or future operator/licensee is requested to justify the adequacy of the SPPA-T2000 hardware development process and lifecycle data.

T15.TO2.41 - SPPA-T2000 Qualification does not address or justify the omission of Accident Radiation, Accident Thermodynamics and Post Accident Conditions tests. The designer or future operator/licensee is requested to ensure that test coverage includes such tests or justify why they are not applicable.

T15.TO2.42 - The SPPA-T2000 Production Excellence strategy has been provided in *UKEPR EPR control and instrumentation (C&I) Actions from Level 4/Level 3 meeting in response to action 33-I&C-6 Letter ND(NII) EPR 00609N*. This production excellence strategy identifies a pre-developed software process review and also states that it has not been performed. The designer or future operator/licensee is requested to perform this review for the UK-EPR.

T15.TO2.43 - The *FA3 standard instrumentation and control system qualification synthesis evaluation report PELL-F DC 52 Rev A* identified a number of test failures. The designer or future operator/licensee is requested to demonstrate/confirm that the modifications made to address these failures are included in the UK-EPR build standard and that the tests on the new UK-EPR standard will be conducted in accordance with IEC61513.

T15.TO2.44 - The IEC 61513 conformance statement presented in section 4 of *IEC 61513 and 62138 justification for SAS, Siemens Energy Sector Document DN 2.2.24 Version 3.0 BP* appears to present a combined conformance statement for the SPPA-T2000 platform and the SAS Application which doesn't clearly differentiate between the two. The designer or future operator/licensee is requested to provide IEC 61513 conformance evidence that clearly differentiates between the SPPA-T2000 platform and Safety Automation System application.

SPPA T2000 Platform – Changing from Version S5

T15.TO1.45 SPPA T2000 - Changing from Version S5

The review of the SPPA-T2000 platform was performed on version S5; however it is believed that an alternative version may be used for UK-EPR.

Should an alternative version of the SPPA-T2000 platform be used for UK-EPR, the designer or future operator/licensee is requested to produce the following:

- A formal change proposal to modify the UK EPR baseline to the alternative version of SPPA-T2000;
- A Basis of Safety Case that as a minimum addresses:

Annex 5

- **How the designer or future operator/licensee will assure at least the same level of platform reliability as that achieved by version S5;**

- **A comprehensive impact assessment of the delta between SPPA-T2000 S5 and the alternative version on the rest of the C&I architecture.**

Review of other Platforms

T15.TO1.46 - Basis of Safety Case for Non Computerised Safety System Platform

Evidence on standards, guidance and criteria that are to be used to demonstrate that the Non Computerised Safety System platform is fit for purpose has not been provided within the timescales of this review.

The designer or future operator/licensee is requested to produce a Basis of Safety Case to demonstrate the adequacy of the safety of the platform used for Non Computerised Safety System.

T15.TO1.47 - Basis of Safety Case for Qualified Display System Platform

Evidence on standards, guidance and criteria that are to be used to demonstrate that the Qualified Display System platform is fit for purpose has not been provided within the timescales of this review.

The designer or future operator/licensee is requested to supply a Basis of Safety Case to demonstrate the adequacy of the safety of the Qualified Display System platform.

T15.TO1.48 - Qualification Method for Smart Devices

It was planned to review EDF and AREVA's position paper that describes the process used for qualification of the smart devices with a reliability claim of 10^{-2} pfd and which also defines complementary measures to be considered for the qualification process of smart devices with a reliability claim of 10^{-3} pfd. However the position paper was not provided by EDF and AREVA within the timescales of this review.

The designer or future operator/licensee is requested to define the methodology used for the qualification of the Smart devices used in nuclear safety functions.

Claims Argument Evidence

A review of the TELEPERM XS and SPPA T2000 evidence which had been identified as part of the Claims Argument Evidence that demonstrates satisfaction of the Safety Assessment Principles was performed. The primary aim of the review was to determine if the evidence cited in *Claims-Argument-Evidences trail for satisfaction of SAPs relevant to I&C PELL-F DC 9 Rev C* supported the claims and arguments.

The following technical observations were made:

T15.TO2.49 - For SAP EDR.1 *Self Test Coverage Analysis SIE QU633 version 7* does not present a system level reliability study for the T2000 platform which is requested to support the fail safe argument. The reliability study is presented in *Reliability Analysis SPPA-T2000 SIE QU627 revision 4.0*. The designer or future operator/licensee is requested to cite the *Reliability Analysis SPPA-T2000*

Annex 5

SIE QU627 revision 4.0 in the version of the claims-argument-evidence that is referenced from the UK EPR pre-construction safety report.

T15.TO2.50 - For SAP EDR.1 the Failure Modes and Effects Analysis for the SDI1-24 Digital Input Module Report (*SDIx Failure Mode and effect analysis (FMEA) NLTCG2008EN1013 Rev B*) as used in the TELEPERM XS shows that there are a number of potential failures that cannot be detected. The designer or future operator/licensee is requested to demonstrate that this level of risk is acceptable.

T15.TO2.51- For SAP EDR.3 the TELEPERM XS Probabilistic Safety Analysis should be referenced by the *Claims-Argument-Evidences trail for satisfaction of SAPs relevant to I&C PELL-F DC 9 Rev C*; The designer or future operator/licensee is requested to include this reference for this SAP in the version of the claims-argument-evidence that is referenced from the UK EPR pre-construction safety report.

T15.TO2.52 - For SAP ESS.23 *Chapter 18.2.4 of the Pre Construction Safety Report PRINCIPLES OF NORMAL OPERATION - Core Unloading* is cited as evidence; this doesn not appear relevant to this SAP. The designer or future operator/licensee is requested to explain the relevance of this reference to this SAP.

T15.TO2.53 - For SAP ESS.27 the evidence *Test Certificate - TXSDRVGEN-0707-02* is cited. The designer or future operator/licensee is requested to update the Claims, Argument and Evidence trail to clarify the purpose of this evidence.

T15.TO2.54 - For SAP EDR.3 the evidence *Protection System, Reliability and availability study NEPS-F DC 29* is cited however it is understood that this document will be superseded by Failure Mode Effects Analysis calculations. The designer or future operator/licensee is requested to update the Claims, Argument and Evidence trail for this SAP to ensure it refers to the document.

T15.TO1.55 - For SAP EDR.2 the cited evidence *SPPA-T2000 reliability analysis for the T2000 SIE QU627 revision 4.0* platform is only hardware based and does not take into account systematic software failure of the platform software. The designer or future operator/licensee is requested to include systematic software failure in the SPPA-T2000 reliability analysis for UK-EPR.

T15.TO2.57 - For SAP EDR.3 the cited evidence *Common Cause Failure Analysis of FA3 I&C Architecture H-P1A-2007-02803-FR May 2009* Section 1 states that the method is qualitative in nature. However it is understood that the results of the CCF analysis are used as inputs to reliability calculations. The designer or future operator/licensee is requested to justify how the results of a qualitative CCF analysis can be used in reliability calculations.

T15.TO2.58 - For SAP EDR.3 the cited evidence *Analysis of the digital CCF within systems supporting F1A safety-class functions (PS) in the instrumentation & control architecture of the FA3 EPR, ENSECC080054 Rev A1* does not address the potential for CCF within TELEPERM XS itself. Although the shared use of software is addressed, there is no discussion on the potential for digital hardware components as a source of CCF. The designer or future operator/licensee is requested to review the potential for CCF of digital hardware components within TELEPERM XS platform itself, and include the evidence in the Claims, Argument and Evidence trail.

T15.TO2.59 - For SAP ESS.27 the response to TATS action 33 I&C 6 which is recorded in *Appendix 1 Production Excellence and Independent Confidence Building Measures strategy for systems supporing F1B function* of EDF and AREVA letter *EPR00609N* should be cited as evidence of Design Production

Annex 5

Excellence for pre-existing T2000 software. The designer or future operator/licensee is requested to update the Claims, Argument and Evidence trail for this SAP as appropriate.

T15.TO2.60 - For SAP ESS.27 and ESR.5 the software re-use argument presented in *IEC 61513 and 62138 justification for SAS, Siemens Energy Sector Document DN 2.2.24 Version 3.0 BPE* should address all class 2 hardware components of the SPPA-T2000 platform that contain dedicated devices with embedded software, or if no such software exists a positive statement saying so should be made. The designer or future operator/licensee is requested to update the Claims, Argument and Evidence trail for this SAP as appropriate.

T15.TO2.61 - For SAP ESS.15 The argument in the Claims Argument Evidence Trail presents the principles for the security procedures that will be used to control access to the SPPA Engineering System. However no argument is presented regarding measures to ensure that the Engineering System cannot cause unintended interference with the class 2 Safety Automation System during plant operation. The designer or future operator/licensee is requested to implement measures that ensure the Engineering System cannot cause unintended interference with the class 2 Safety Automation System during plant operation.

T15.TO2.62 – Some Failure Modes and Effects Analysis for TELEPERM XS components have been provided e.g. *Failure modes, failure effect and failure detection SVE2, NLTC-G/2008/en/1010* and *SDIx Failure Mode and effect analysis (FMEA) NLTCG2008EN1013 Rev B*. The designer or future operator/licensee is requested to include Failure Modes and Effects Analysis for all TELEPERM XS components applicable to the UK-EPR in the CAE trail.

Review of the actions identified in United States Nuclear Regulatory Commission Safety Evaluation Report "Teleperm XS: A digital Reactor Protection System"

The TSC Task 15 review considered the observation raised in paragraph 39 of the *Nuclear Directorate – Generic Design Assessment – New Civil Reactor Build - Step 3 Control and Instrumentation Assessment of the EDF and Areva UK EPR, Division 6 Assessment Report No. AR 09/038-P.* Paragraph 39 states:

> *"The United States Nuclear Regulatory Commission (US NRC) has completed a safety evaluation of the Teleperm XS platform and the safety evaluation report will be considered during our Step 4 assessment."*

The report *United States Nuclear Regulatory Commission Safety Evaluation by the Office of Nuclear Reactor Regulation Siemens Power Corporation Topical Report EMF-2110 (NP), "Teleperm XS: A digital Reactor Protection System" Project No. 702. Dated 5th May 2000* identifies 17 actions, 4 of which (1, 12, 13 and 17) have been investigated during this review as they aligned with some of the review activities performed under TSC Task 15. The remaining 13 actions have been reviewed by other TSC tasks. The review identified 8 TSC Task 15 technical observations that relate to the 4 Nuclear Regulatory Commission actions. The associated TSC Task 15 observations are:

- T15.TO2.12;
- T15.TO2.13;
- T15.TO2.14;

Annex 5

- T15.T02.30;
- T15.T02.31;
- T15.T02.32;
- T15.T02.33;
- T15.T02.58.

In conclusion it is the opinion of the TSC that from the evidence sampled that:

For the TELEPERM XS platform version 3.5.3:

- The review performed to determine the adequacy and sufficiency of the samples of evidence provided by the Requesting Party to support claims and arguments of the application of appropriate standards and guidance to the production of the platform identified four major areas for improvement regarding:
    - Justification for the use of Programmable Complex Electronic Components in TELEPERM XS modules for deployment in Class 1 C&I Systems;
    - Role of the External Independent Assessor in Software Production Excellence and Independence Confidence Building Measures;
    - Role of the External Independent Assessor in Hardware Development and Verification Activities;
    - Provision of a Basis of Safety Case for Qualified Display System Platform.
- The review performed to determine from the samples of the evidence provided by the Requesting Party that the functionality and performance of the TELEPERM XS platform are adequate and sufficient for deployment in a Class 1 system (through a focused review of Deterministic Behaviour, Self Checking and Fault Management) identified no major areas of improvement.

From the evidence sampled and subject to successful resolution of all technical observations related to the TELEPERM XS platform no evidence was found to indicate that the TELEPERM XS platform version 3.5.3 is not adequate and sufficient for deployment in a Class 1 system.

For the SPPA-T2000 version S5:

- The review performed to determine the adequacy and sufficiency of the samples of evidence provided by the Requesting Party to support claims and arguments of the application of appropriate standards and guidance to the production of the platform identified three major areas for improvement regarding:
    - Adequacy of Testing and Test Evidence;
    - Evidence of the application of IEC 60987 to hardware development of the SPPA-T2000;
    - Potential change from SPPA-T2000 version S5 for UK EPR.

From the evidence sampled and subject to successful resolution of all technical observations related to the SPPA-T2000 platform no evidence was found to indicate that the SPPA-T2000 platform version S5 is not adequate and sufficient for deployment in a Class 2 system. However it should be noted that

Annex 5

should a different version of SPPA-T2000 be used on UK EPR then the designer or future operator/licensee is requested to demonstrate that the selected version is adequate and sufficient for deployment in a Class 2 system.

For the NCSS only the functional and safety requirements and diversity criteria were available during the timescales of the review and these were addressed by TSC Task 20 that reviewed the responses to Regulatory Issue RI-UKEPR-002 actions A1.2 and A1.3. No opinion on the NCSS platform can be formed until the standards, guidance and criteria used for platform production have been demonstrated as adequate and sufficient for deployment in a Class 2 system.

For Smart Devices, no opinion can be formed until details of the methodology used for the qualification of the Smart devices used in safety functions has been provided and reviewed.

Annex 6

Review of C&I Safety and Safety Related Systems – TSC Summary[7]

Note this information has been imported from a TSC report (Ref. 31) and the formatting of the TSC report has been retained.

[7] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 6

A Annex: TSC Task Summary: Review of C&I Safety and Safety-Related Systems

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of Safety and Safety-Related Systems for UK EPR for the UK EPR reactor design.

This review follows on from the review of process-related claims and argumentation carried out in a preliminary activity (TSC Task 6). The aim of the review has been to gain confidence that the Requesting Party (Electricité de France SA and Areva NP SAS, hereafter referred to as "EDF and AREVA") have adequate evidence to demonstrate that appropriate standards have been conformed to in the development of Safety and Safety-Related Systems for UK EPR, and the principles of production excellence and independent confidence building measures have been applied in the development of the software in Class 1 systems. This has included a review of samples of the evidence to support further claims and argumentation presented by EDF and AREVA relating to relevant Safety Assessment Principles (SAPs) and international nuclear standards. Due cognisance has been taken of selected Technical Assessment Guides (TAGs).

The task has also reviewed samples of the evidence presented by EDF and AREVA via:

- the claims-argument-evidence table that provides the RP's basis of the demonstration of SAP conformance;
- responses to Technical Queries;
- responses to actions from meetings involving EDF and AREVA, HSE/NII and the TSC
- and responses to technical observations raised during the preliminary activity, including system-related observations in the HSE/NII GDA Step 2 and 3 reports.

The systems that were originally within the scope of the task were the Protection System (PS), the Safety Information and Control System (SICS), the Safety Automation System (SAS) and the Process Automation System (PAS). One further system was added to the architecture as part of the response to Regulatory Issue RI-UKEPR-02 – the Non-Computerised Safety System (NCSS) – but evidence relating to the safety demonstration of this system has not been presented in the timeframe of this review. The inclusion of the Qualified Display System (QDS) has been proposed for addition to the C&I architecture. However the details of the implementation of this system, including provision of a safety demonstration, through a Basis of Safety Case (Safety Plan, Safety Deliverables, Schedule and argument that demonstrates the deliverables meet the requirements of the applicable standards and SAPs), has not been presented in the timeframe of this review.

The scope of the evidence that is specific to the UK EPR is defined by EDF and AREVA in *"UK EPR CONTROL AND INSTRUMENTATION (C&I) – SCOPE OF GDA"* (letter ND (NII) EPR00686N). As some UK EPR evidence, including function block diagrams, was not available within the timeframe of this review, some of the reviews (e.g. design documents, PS function block diagrams) were based on evidence from the Flamanville 3 (FA3) C&I system. EDF and AREVA have indicated that improvements to the processes for requirements definition and traceability used in the development of FA3 have already been identified. Not all of the UK EPR evidence that has been declared in scope and was to be considered within the selected sample has been provided within the timescale of this review.

The observations in the HSE/NII reports for GDA Steps 2 and 3 have been apportioned for review to tasks 14 through 18.

Annex 6

Of the 7 observations in the Step 2 report that were apportioned to this task, 1 is considered by the TSC to be resolved. Some progress has been made on the other 6 observations. Outstanding points are covered by the following Technical Observations (TOs) and potential GDA Issue (pGI) which have been raised in relation to them: T16.TO1.02, T16.TO1.03, T16.TO2.18, T16.TO2.22, T16.TO2.26, pGI-UKEPR-C&I.07.02[8]. The original Step 2 observations are adequately addressed by these TOs and pGI.

Only one observation of the Step 3 report (in paragraph 39) was apportioned to this task. It states that the actions identified in the safety evaluation report produced by United States Nuclear Regulatory Commission (US NRC) will be considered during the Step 4 assessment. The Task 16 review of samples of the evidence provided by EDF and AREVA has led to the following conclusions for these US NRC actions:

- **Action 2**: Verification and Validation, and configuration management activities have been considered as part of the Task 16 review. Further evidence is needed to demonstrate that the activities are conformant to nuclear standards (See T16.TO1.01). Based on the sampled evidence reviewed there are some areas for improvement with V&V activities (See T16.TO2.19). Based on the sampled evidence, no areas for improvement have been identified with system configuration management activities.

- **Action 9**: The Fault Schedule (PEPR-F DC 4 B) includes a worksheet which shows which functions reduce the risk from anticipated transients without scram (ATWS). However, it does not identify diverse means for providing the protection (See T16.TO2.21).

- **Action 17**: EDF and AREVA has improved the process for managing traceability data. However, a method document that defines how traceability data is managed has yet to be produced (T16.TO2.15).

The original Step 3 actions are adequately addressed by the referenced TOs.

Regarding standards conformance, selected IEC standards have provided a reference for this part of the review. For the PS, EDF and AREVA has committed to provide analyses which demonstrate compliance with specific IEC standards (i.e. General Requirements for Systems IEC 61513:2001, Class 1 and 2 Hardware Requirements for Computer Based Systems IEC 60987:2007 and Software Requirements for Systems Performing Category A Functions IEC 60880:2006) but the delivery dates are too late for consideration in this review (see T16.TO1.01). In the absence of such analyses, samples of other project evidence, such as quality plans have been reviewed against the requirements of the standards. Based on the evidence sampled, no major areas for improvement in standards conformance for the Protection System have been identified. However a number of detailed technical observations have been raised.

Regarding independent confidence building measures (as specified in ESS.27), for the PS software, quality assessments of system documents are performed by EDF independent units (e.g. SEPTEN and CEIDRE). Also, on-site commissioning tests that exercise all C&I equipment and systems are to be carried out by EDF and AREVA. Additionally, EDF and AREVA has committed to:

[8] ND note: GI-UKEPR-CI-06.A2 is the issued version of the provisional GDA Issue (pGI).

Annex 6

- produce a feasibility study on static analysis of the UK EPR Protection System software, and the qualification of the TELEPERM XS development tools, including the automatic code generator and C compiler and
- carry out a minimum of 5000 tests on the TELELEPRM XS PS Test Division, and to carry out a review of the reasonable practicability of carrying out additional tests (up to 50,000) within the PS implementation programme. Research will be undertaken into the feasibility of implementing statistical testing on simulation of the PS using the simulator (SIVAT).

For the SAS and PAS the evidence for compliance with IEC 61513:2001 and IEC 62138:2004 was presented through various quality plans. Based on the evidence sampled, no major areas for improvement in standards conformance for the SAS and PAS have been identified. However a number of detailed technical observations have been raised with respect to identification of evidence to substantiate the compliance claims. EDF and AREVA has committed to provide an analysis which demonstrates compliance with IEC 60987:2007 but have declared this to be out of scope of GDA.

Regarding demonstration of compliance with the selected SAPs via the claims-argument-evidence information, no major areas for improvement have been identified. However a number of detailed technical observations have been raised.

A total of 34 technical observations have been raised from this review. These technical observations have been designated TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher – 3 of these have been designated TO1 and the remainder have been designated TO2.

The TO1 technical observations are:

1. **T16.TO1.01** - The designer or future operator/licensee is requested to demonstrate that the processes to develop the Protection System (PS) are compliant with:

   - IEC 61513:2001
   - IEC 60880:2006
   - IEC 60987:2007

   Regarding IEC 61513: 2001, it is noted that table 7 of the System Quality Plan (SQP) (NLE-F DM 10007, Revision D) provides a top level mapping between clauses in the standard and process steps defined by the SQP. Although informative, it does not provide sufficient detail to confirm that all aspects of each clause, as specified by detailed sub-clauses, are satisfied. The designer or future operator/licensee is requested therefore to ensure that the analysis addresses the detailed sub-clauses.

2. **T16.TO1.02** - The designer or future operator/licensee is requested to demonstrate the safety of the Non-Computerised Safety System, through a Basis of Safety Case (Safety Plan, Safety Deliverables, Schedule and argument that demonstrates the deliverables meet the requirements of the applicable standards and SAPs), to include evidence that the processes to develop the equipment will be compliant with appropriate standards including:

   - IEC 61513:2001

Annex 6

- IEC 60987:2007

3. **T16.T01.03** - The designer or future operator/licensee is requested to demonstrate the safety of the Class 1 displays, through a Basis of Safety Case (Safety Plan, Safety Deliverables, Schedule and argument that demonstrates the deliverables meet the requirements of the applicable standards and SAPs), to include evidence that the processes to develop the application and the equipment will be compliant with appropriate standards such as:

   - IEC 61513:2001
   - IEC 60880:2006
   - IEC 60987:2007

The T02 technical observations applicable to the Protection System are:

1. **T16.T02.10** - Table 2 of the SQP (NLE-F DM 10007, Issue D) defines the engineering documents that are to be produced. The scoping letter (Scope of UK EPR Instrumentation & Control Design for GDA, ND (NII) EPR00686N, 22 December 2010) states the development phase 'System Specification' is within scope of GDA. However, the following documents which are produced by that phase have not been provided:

   - D-01.3: Master Test Plan
   - D-01.4: Protection System - System Requirements Specification
   - D-01.5: System Qualification Plan
   - D-01.9: System Configuration Management Plan
   - D02.3: Protection System - System Functional Design Description

   The designer or future operator/licensee is requested to ensure UK EPR versions of the above documents are produced.

2. **T16.T02.11** - In the absence of provided compliance analyses to demonstrate the satisfaction of the requirements of IEC 60987:2007 for the protection system, conformance has been considered by the review of samples of other project evidence, such as quality plans and a number of detailed points have been raised.

   The designer or future operator/licensee is requested to address the following points related to project quality plans:

   a. Clause 5.3.6 requires maintenance requirements to be specified. There is no indication in the provided evidence of how this requirement is satisfied.
   b. Clause, 5.4.4 requires that hardware requirements identify prohibited construction materials or production processes. There is no indication in the provided evidence of how this requirement is satisfied.

3. **T16.T02.12** - Table 8 of a previous version of the quality plan (NLE-F DC 113, Issue C) identified the Method Documents which are relevant to individual process steps. Table 8 of the UK EPR

Annex 6

quality plan (NLE-F DM 10007, Issue D) only lists Method Documents but does not indicate which process step they are applicable to.

It therefore cannot be confirmed that all process steps have an associated Method Document.

The designer or future operator/licensee is requested to demonstrate that all process steps have adequate detailed procedures, which provide the necessary rules and guidelines to be followed when the process steps are being undertaken.

4. **T16.T02.13** - Guidelines for the Verification of TELEPERM XS Application Software Items (NLE-F, DM 10022) is under development.

   The designer or future operator/licensee is requested to review this document and confirm its adequacy.

5. **T16.T02.14** - The user manual for developing TELEPERM XS-based applications is entitled 'TELEPERM XS User Manuals, Engineering System SPACE. TXS-2100-76-V4.0'.

   The following areas for improvement have been identified in relation to this document:

   a. There is no reference to the user manual from the System Quality Plan (SQP) for TXS C&I applications (NLE-F DM 10007, Revision D). The designer or future operator/licensee is requested to demonstrate that due account is taken of the manual in the development of TELEPERM XS based applications.

   b. It is noted that the manual specifically refers to version 3.4.x of the Core Software. The Technical Support Contractor understands that the core software is at a later release (3.5.x).

      The designer or future operator/licensee is requested to demonstrate that development of UK EPR TELEPERM XS-based applications is based on a version of the TELEPERM XS User Manual which is applicable to the version of TELEPERM XS that is selected for the UK EPR.

6. **T16.T02.15** - The process to manage traceability data from requirements through design and implementation, and to Verification and Validation (V&V) is still under development, and no traceability data has been provided for the UK EPR.

   The designer or future operator/licensee is requested to:

   a. Ensure a method document that defines how traceability data is managed is produced.

   b. Ensure evidence of comprehensive traceability from input requirements through to System Requirements, software and hardware requirements, design and implementation, and V&V evidence is produced.

7. **T16.T02.16** - IEC 60880:2006, clause 12.4.2 requires training plans to be developed. This is not addressed by the System Quality Plan (SQP) (NLE-F DM 10007, Issue D). EDF and AREVA have stated that production of training plans is outside the scope of the SQP. The Overall C&I System Quality Plan (NLN-F DC 132, Rev A) has been inspected and this does not address Training Plans.

   The designer or future operator/licensee is requested to ensure that the requirement to produce Training Plans is in scope of an appropriate controlling document such as a quality plan.

Annex 6

8. **T16.T02.17** - The following areas for improvement regarding the use of TELEPERM XS development and verification tools have been identified:

   a. An observation was raised as part of a preliminary activity known as Task 6 concerning the potential risk of faults being introduced through the use of TELEPERM XS tools.

      The response was, in summary, that the qualification of tools is addressed as part of the development of the TELEPERM XS platform.

      However, the response does not address the original observation, which is over how the tools are used and whether or not the development process includes measures which mitigate faults which might be introduced through their use (e.g. verification of tool outputs). So risks associated with tool usage are specific to the process used to develop applications, and the generic argument that the tools have been qualified is insufficient.

      The designer or future operator/licensee is requested to demonstrate that:

      - The way tools are used to develop and verify applications has been analysed to mitigate potential faults that might be introduced.
      - Restrictions on the way tools should be used are considered and addressed in the development process.

   b. The 'CASSIS' tool is used during testing to identify discrepancies between expected and actual results, which are subsequently analysed manually. This indicates that the V&V process is dependent on the integrity of this tool.

      The designer or future operator/licensee is requested to demonstrate that the CASSIS tool is of adequate integrity for the verification of Class 1 applications.

   c. The SPYCE tool performs syntactic checks of the SPACE Database.

      The designer or future operator/licensee is requested to demonstrate that the SPYCE tool is of adequate integrity for its use in verifying the SPACE database.

9. **T16.T02.18** – Regarding error detection and management within the Protection System, if a function block detects that one of its inputs is out of range, the output is set to an extreme value, but the corresponding fault flag is not set. Therefore when the output is used as an input to a subsequent function block it would not be aware that an error had occurred.

   The designer or future operator/licensee is requested to ensure errors are handled appropriately (e.g. errors detected inside function blocks are communicated to subsequent function blocks, and managed in subsequent function blocks.)

10. **T16.T02.19** – The following areas for improvement have been identified regarding testing of the Protection System:

    a. Test coverage is in the form of requirements coverage. It is demonstrated within test specifications (D-03.2), which provide traceability between test cases and functions defined by document D-02.3.

       However, there is no structural coverage information to explain how the paths in the following documents are tested:

       - D-21.1: I&C Function Specification

Annex 6

- D-22.1: Function Diagrams (i.e. Specification and Coding Environment (SPACE) Diagrams)

The designer or future operator/licensee is requested to ensure adequate structural test coverage at the function block level is recorded in an auditable form.

b. Some testing is performed using the Simulation Based Validation Tool (SIVAT). The Technical Support Contractor has noted that the object code tested on the simulator will be different from that executed on the target, because different compilers are used.

EDF and AREVA have explained that for individual function blocks this would not be an issue, as the entire function block library will have been tested on the target as part of the TELEPERM XS development, and delivered as object code (as opposed to being recompiled for the application). However, the application will contain calls into the function block library, and the object code for these calls tested on SIVAT will be different from the target object code.

The designer or future operator/licensee is requested to demonstrate that the testing of the object code of the Protection System, either via the verification and validation process or via the statistical testing activity, achieves adequate coverage (e.g. statements, branches and path segments) of the object code of the executable application program.

11. **T16.T02.20** - The C&I TXS Cabinets Qualification Program (NLZ-F DC 3, Revision C) has been reviewed and a number of areas for improvement have been identified. The designer or future operator/licensee is requested to address the following observations:

    a. It appears from the System Quality Plan (SQP) (NLE-F DM 10007, Issue D) that the System Requirements Specification encapsulates the Performance Specification; however there is insufficient provided information to determine if it addresses the requirements of clause 5.2 of IEC 60987.

    b. Section 7 of the TXS Cabinets Qualification Program states that tests will be performed across a range of environmental conditions, by reference to 'Design and Construction Rules for Electrical Components of Nuclear Islands, December 2005' (RCC-E). However exposure to radiation and chemicals are not addressed (as required by IEC 60780 clause 5.3.1.5.)

    c. Clause 5.3.2 of IEC 60780:1998 states that tests for accident conditions should be performed, including earthquake, cumulated irradiation doses, injection of saturated steam. Section 7.5.2 of the qualification plan addresses seismic tests, but no tests were presented for other accident conditions.

12. **T16.T02.21** - This concern was originally raised in paragraph 39 of the observations that relate to C&I Class 1 and more important Class 2 systems, that are raised in the HSE/NII report for GDA Step 3 C&I assessment of the UK EPR design.

    The Fault Schedule (PEPR-F DC 4 B) includes a worksheet which shows which functions reducing the risk from anticipated transients without scram (ATWS). However, it does not identify diverse means for providing the protection.

Annex 6

The designer or future operator/licensee is requested to demonstrate that the TXS system is diverse from the system for reducing the risk from anticipated transients without scram (ATWS).

13. **T16.TO2.01** - The designer or future operator/licensee is requested to address the following observations which have arisen from the review of the Claims/Argument/Evidence (CAE) information presented by EDF and AREVA to support conformance to SAP EQU.1 (Equipment qualification):

    a. The argument states that qualification procedures will address actuators, sensors and essential services. However, qualification of these items is not addressed by the referenced evidence (NLE-F DC 113 "TXS based I&C System Quality Plan, NLZ-F DC 3 "I&C TXS cabinets Qualification Program").

       The designer or future operator/licensee is requested to update the CAE to demonstrate that adequate qualification procedures are established for actuators, sensors and essential services.

    b. The CAE refers to the TXS based C&I System Quality Plan as NLE-F DC 113, but that document has been superseded by NLE-F DM 10007.

       The designer or future operator/licensee is requested to:

       - Update the CAE to refer to NLE-F DM 10007 rather than NLE-F DC 113.
       - Review the CAE, and update if necessary, to ensure that it includes correct document references.

    c. The CAE does not address qualification of the TXS components.

       The designer or future operator/licensee is requested to update the CAE to demonstrate that the TXS components have been adequately qualified.

    d. The designer or future operator/licensee to note that a number of areas for improvement relating to TELEPERM XS equipment qualification were identified as a result of the review of evidence against standards, and those points are applicable to the CAE presented for SAP EQU.1. (See T16.TO2.20 above).

       The designer or future operator/licensee is requested to update the CAE for EQU.1 to address the areas for improvement reflected in T16.TO2.20.

    e. RCC-E defines the French design and construction rules for electrical components of nuclear islands, and EDF and AREVA have claimed compliance with these rules. In particular, NLZ-F DC 3 "I&C TXS cabinets Qualification Program" indicates that various chapters within RCC-E will be satisfied (e.g. B2400, B2500, B2600). However, a number of other chapters (e.g. B2240, B2300 and B3500) also contain requirements related to equipment qualification, but these chapters are not discussed in the evidence.

       The designer or future operator/licensee is requested to review the CAE, and update it to ensure it fully addresses the requirements of RCC-E.

    f. RCC-E chapters B5000 and B6000 include qualification requirements for equipment in *'ambience family 1 and 2'* respectively. The evidence does not state which family the cabinets belong to, nor does it confirm that the appropriate requirements are satisfied.

Annex 6

The designer or future operator/licensee is requested to update the CAE to state which '*ambience family*' the cabinets belong to, and demonstrate that the appropriate requirements are satisfied.

14. **T16.T02.02 -** This TO was raised in error in an early draft of the report, and was subsequently removed.

15. **T16.T02.03 -** The designer or future operator/licensee is requested to address the following observations which have arisen from the review of the Protection System CAE information presented by EDF and AREVA to support conformance to SAP EDR.2 (Design for Reliability - Redundancy, diversity and segregation), and update the CAE information:

    a. The referenced evidence (Protection System Detailed Specification file, NLE-F DC 38) has been superseded by NLN-F DC 193, Rev A (Protection System-System description).

       The designer or future operator/licensee is requested to:

       - Update the CAE to refer to NLN-F DC 193 rather than NLE-F DC 38.
       - Review the CAE, and update if necessary, to ensure that it includes correct document references.

    b. Section 4.2 of NLE-F DC 249, Revision C, ("TELEPERM XS based systems Concept for Electrical Separation") states that the technical solutions are temporary, and the analysis is in progress. Completeness of the analysis for the UK EPR needs to be confirmed.

       The designer or future operator/licensee is requested to update the CAE to demonstrate that an analysis of the UK EPR architecture has been performed.

    c. Appendix A of NLE-F DC 249, Revision C identifies the signal exchanges and states whether segregation between systems, through separation or decoupling, is implemented for each. The following points are noted:

       - For some signal exchanges it is concluded that there is no need for separation or decoupling, but no justification is provided.
       - Not all signal exchanges between modules of the Protection System are addressed e.g. it does not address Remote Acquisition Unit / Acquisition and Processing Unit, Acquisition and Processing Unit / Actuator Logic Unit

       The designer or future operator/licensee is requested to update the CAE to demonstrate adequacy of segregation of all signal exchanges between modules of the Protection System. This should include justifications for those cases where there is no separation or decoupling.

    d. The evidence does not address physical separation of cables as required by RCC-E, chapter D7300.

       The designer or future operator/licensee is requested to update the CAE to demonstrate adequacy of separation of cables, as required by RCC-E, chapter D7300.

16. **T16.T02.04** - The designer or future operator/licensee is requested to address the following observations which have arisen from the review of the Protection System CAE information

Annex 6

presented by EDF and AREVA to support conformance to SAP EDR.3 (Design for Reliability - Common Cause Failure (CCF)), and update the CAE information:

a. Section 1 of H-P1A-2007-02803-FR ("I&C Electrical Systems Project: Common Cause Failure Analysis of FA3 I&C Architecture") explains that the analysis only considers designs of digital components or systems as sources of CCF. The justification is that other sources of CCF are taken into account in the design of the system. However, there is no reference to an analysis of Common Cause Failure of non digital aspects of the system (e.g. electrical power.)

   The designer or future operator/licensee is requested to update the CAE to demonstrate that an adequate Common Cause Failure analysis has been performed on non digital aspects of the system.

b. Section 1 of H-P1A-2007-02803-FR states that the method for CCF analysis is qualitative in nature. However it is understood that the results of the Common Cause Failure analysis are used as inputs to reliability calculations. Clarification is needed on how the Common Cause Failure analysis supports the reliability calculations.

   The designer or future operator/licensee is requested to update the CAE to clarify how the qualitative nature of the Common Cause Failure analysis supports the reliability calculations.

c. The potential for Common Cause Failure within TELEPERM XS itself is not fully addressed, in that although the shared use of software is considered, there is no discussion on the potential for digital hardware components as a source of Common Cause Failure.

   The designer or future operator/licensee is requested to update the CAE to demonstrate that adequate consideration has been given to the potential for digital hardware components as a source of Common Cause Failure.

d. The argument states that the shared use of subroutines within TXS is addressed in the "non-specific processing part" of the C&I compact model used in the Probabilistic Safety Assessment (PSA). This is documented in section 4.3.14.3 of the PSA (NEPS-F DC 355) which supports the argument. The PSA should therefore be referenced from the argument.

   The designer or future operator/licensee is requested to update the CAE to include the PSA as part of the argument.

e. Section 4.4 of ENSECC080054 ("Analysis of Digital Common Cause Failures of E1A (PS) Class Level 1 Systems of FA3 I&C Architecture") states that network bandwidth between divisions is a potential source of Common Cause Failure. It goes on to describe mechanisms within TXS which ensure that saturation of one network cannot affect others. However this only addresses networks within a division, and not across divisions. Further evidence is needed to demonstrate cross division networks have been analysed as potential sources of Common Cause Failure.

   The designer or future operator/licensee is requested to update the CAE to demonstrate that adequate consideration has been given to the potential for networks between divisions as sources of Common Cause Failure.

f. The independence of the networks within a division has been investigated (by the Technical Support Contractor) by considering the architecture as described in the PS System Description, NLN-F DC 193. It is noted not all networks within the Protection

Annex 6

System are considered within the analysis (e.g. Remote Acquisition Unit / Acquisition and Processing Unit; Acquisition and Processing Unit/ Actuator Logic Unit). The analysis should be updated to consider all networks.

The designer or future operator/licensee is requested to update the CAE to demonstrate that the CCF analysis addresses all networks within the Protection System.

g. The argument states that shared use of hardware / equipment (cabinets, cabling, piping, power etc); Sensors; Actuators are addressed by the evidence. However, the referenced evidence does not address these.

The designer or future operator/licensee is requested to update the CAE to demonstrate that CCF analysis addresses all hardware / equipment (cabinets, cabling, piping, power etc), Sensors and Actuators.

17. **T16.T02.05** - The designer or future operator/licensee is requested to address the following observations which have arisen from the review of the Protection System CAE information presented by EDF and AREVA to support conformance to SAP EMT.7 (Maintenance, Inspection and Testing - Functional Testing), and update the CAE information:

a. The CAE refers to NLE-F DC 38 (PS Detailed Specification File) which is a Flamanville 3 document. The evidence needs to be updated for UK EPR.

The designer or future operator/licensee is requested to update the CAE to address the UK EPR architecture.

b. It is noted that the test approach for safety functions is performed in discrete stages, e.g. verify that sensor data is acquired by the Protection System; verify that trip signals from the Actuator Logic Unit activate Reactor Trip, through the use of test signals.

This approach does not seem to be consistent with the requirements of the SAP and RCC-E Chapter C3323, which imply that complete functions should be tested.

The designer or future operator/licensee is requested to update the CAE to demonstrate that complete functions are tested, as required by the SAP and RCC-E Chapter C3323.

c. RCC-E chapter C3322 states '*When a trip parameter is computed from several variables, the contribution of each variable shall be verified individually, with the other variables adjusted to within their operating range at a nominal or at a preset value*.' The evidence referenced in the CAE trail does not demonstrate that this requirement is satisfied.

The designer or future operator/licensee is requested to update the CAE to demonstrate that the requirements of RCC-E chapter C3322, concerning the contribution of individual variables to trip parameter calculations, are satisfied.

d. Chapter C3323 of RCC-E states that test signals shall be superimposed on normal signals (thus perturbing the measured variable), or by using a substitute input signal. There is no provided evidence of this principle being applied.

The designer or future operator/licensee is requested to update the CAE to demonstrate that the requirements of RCC-E chapter C3323, concerning the imposition of test signals on normal signals, are satisfied.

e. Chapter C3322 of RCC-E states that testing of response times is not needed if it can be checked during plant operation or during routine testing, and if it can be demonstrated that changes in response time beyond reasonable limits are accompanied by detectable

Annex 6

deviations in performance characteristics. This requirement has not been addressed in the CAE information for conformance to EMT.7.

The designer or future operator/licensee is requested to update the CAE to demonstrate that the requirements of RCC-E chapter C3322 regarding the testing of response times are satisfied.

f. Clause 4 IEC 60671:2007 states that failure modes not revealed by self-supervision, shall either be shown not to affect the safety function, or shall be covered by periodic testing. There is no analysis provided, or referred to that demonstrates that periodic testing addresses all failure modes which are not addressed by self-monitoring.

The designer or future operator/licensee is requested to update the CAE to demonstrate that periodic testing addresses all failure modes which are not addressed by self-monitoring, as required by Clause 4 IEC 60671:2007.

g. A number of detailed observations related to the completeness of test definitions, and definition of pass/fail criteria have been identified with the tests listed below.

- Section 2.2.4 states SICS Reactor Trip manual command is not represented since the implementation of the command is not fixed
- Test Principle 3 - step 2 says verify that the test has been correctly performed, without saying how or by providing pass/fail criteria.
- Test Principle 6 (Diesel Standing Order) is not defined.
- Test Principle 11 (analog and digital indicators) indicates that principles have not been defined
- Test Principle 15 (Parameterisation, Test/Diagnosis, Disable Keys) – it is stated that these are tested when used, however no justification is provided. The concern is how it can be confirmed that the functions will be available when required.
- Test Principle 16 'The test is a spot check' suggesting a degree of informality.

The designer or future operator/licensee is requested to update the tests identified above to ensure that they are completely and formally defined.

18. **T16.T02.06** - The designer or future operator/licensee is requested to address the following observations which have arisen from the review of the Protection System CAE information presented by EDF and AREVA to support conformance to SAP ESS.18 (Safety Systems - Failure Independence), and update the CAE information.

a. Section 4.2 of NLE-F DC 249, Revision C, ("TELEPERM XS based systems Concept for Electrical Separation") states that the technical solutions for separation are temporary, and the analysis of compliance with RCC-E is in progress. Completeness of the analysis for the UK EPR needs to be confirmed.

The designer or future operator/licensee is requested to update the CAE to demonstrate that an analysis of the UK EPR architecture has been performed.

Annex 6

b. Appendix A of NLE-F DC 249, Revision C identifies the signal exchanges and states whether segregation between systems, through separation or decoupling, is implemented for each. The following points are noted:

- For some signal exchanges it is concluded that there is no need for separation or decoupling, but no justification is provided.
- Not all signal exchanges between modules of the Protection System are addressed.

The designer or future operator/licensee is requested to update the CAE to demonstrate the adequacy of segregation of all signal exchanges between modules of the Protection System. This should include justifications for those cases where there is no separation or decoupling.

c. The referenced evidence does not address separation between modules of the PS, and between cables associated with the PS.

The designer or future operator/licensee is requested to update the CAE to demonstrate adequacy of separation between modules of the PS and between cables associated with the PS. This should include justifications for those cases where there is no separation or decoupling.

d. The referenced evidence does not address the potential for faults with the Service Unit causing the disabling of the PS (e.g. an invalid input from the service unit to the PS).

The designer or future operator/licensee is requested to update the CAE to demonstrate that potential faults with the Service Unit cannot cause the PS to be disabled.

e. The inclusion of the Qualified Display System (QDS) has been proposed for addition to the PS, however no details have been provided in the Step 4 GDA timeframe. If the QDS is included in the PS then the CAE trail will have to be updated to demonstrate that any faults it causes cannot disable the PS.

If the QDS is included within the PS architecture the designer or future operator/licensee is requested to update the CAE to demonstrate that potential faults with the QDS cannot disable the PS.

19. **T16.T02.07** - The areas for improvement described in Technical Observation T16.T02.18 above (concerning error detection and management) are applicable to ESS.21 (Safety Systems – Reliability).

The designer or future operator/licensee is requested to update the CAE for ESS.21 to address the areas for improvement presented in T16.T02.18.

20. **T16.T02.08** - The designer or future operator/licensee is requested to address the following point which has arisen from the review of the Protection System CAE information presented by EDF and AREVA to support conformance to SAP ESS.23 (Safety Systems - Allowance for unavailability of equipment), and update the CAE information.

a. The argument does not refer to the 4-train architecture, which would appear to contribute to the satisfaction of this SAP.

The designer or future operator/licensee is requested to consider the appropriateness of the 4-train architecture in the context of this SAP and update the CAE accordingly

Annex 6

b. The only evidence referred to from the CAE is to chapter 18.2.4 of the PCSR which is not related to this SAP.

The designer or future operator/licensee is requested to update the CAE to demonstrate that the requirements of ESS.23 are satisfied.

21. **T16.T02.09** - The designer or future operator/licensee is requested to address the following observations which have arisen from the review of the Protection System CAE information presented by EDF and AREVA to support conformance to SAP ESS.27 (Safety Systems - Computer-based safety systems), and update the CAE information.

a. The CAE refers to the TELEPERM XS based C&I System Quality Plan as NLE-F DC 113, but that document has been superseded by NLE-F DM 10007. The designer or future operator/licensee is requested to:

- Update the CAE to refer to NLE-F DM 10007 rather than NLE-F DC 113.
- Review the CAE, and update if necessary, to ensure that it includes correct document references.

b. Technical Observations T16.T01.01 and T16.T02.12 through T16.T02.19 are also applicable to this SAP. The designer or future operator/licensee is requested to update the CAE for ESS.27 to address the points recorded in T16.T01.01 and T16.T02.12 through T16.T02.19.

c. Regarding Independent Confidence Building Measures, EDF and AREVA have committed to carry out a minimum of 5000 tests on the TELEPERM XS PS Test Division, and to carry out a review of the reasonable practicability of carrying out additional tests (up to 50,000) within the PS implementation programme. Research will be undertaken into the feasibility of implementing statistical testing on simulation of the PS using the simulator (SIVAT). They have also committed to produce a feasibility study on static analysis of the UK EPR Protection System software, and qualification of the TELEPERM XS development tools, including the automatic code generator and C compiler. This concern is being tracked through pGI-UKEPR-C&I.03.01[9]. However the measures described above are not recorded in the CAE.

The designer or future operator/licensee is requested to update the CAE to include the above information on Independence Confidence Building Measures.

d. The CAE leads to document NLE-F DC 222 - Protection System, Severe Accident I&C, Reactor Control Surveillance and Limitation System V&V and Test Plan as evidence of independent confidence building measures. However, the document describes processes which are required by IEC 60880, and do not represent Independent Confidence Building Measures (i.e. in addition to that required by IEC 60880).

The designer or future operator/licensee is requested review the appropriateness of NLE-F DC 222 in the CAE trail for this SAP, and update the CAE to explain its relevance to Independent Confidence Building Measures.

22. **T16.T02.33** - The designer or future operator/licensee is requested to demonstrate that adequate measures are in place to address the potential design and implementation issues

[9] ND note: GI-UKEPR-CI-02 is the issued version of the provisional GDA Issue (pGI).

Annex 6

concerned with Calculated Trips, which are captured in '*Programmable Calculated Trips – WPD Notes & Checklist* S.P1440.74.11', which is based on requirements and guidance identified in:

- IEC 61513:2001
- IEC 60880:2006
- IEC 61888:2002
- Trip Parameter Acceptance Criteria for Safety Analysis of CANDU Nuclear Power Plants, Canadian Nuclear Safety Commission Regulatory Guide G-144
- IEEE Standard 754 on Floating Point Numbers and Guidance material
- Relevant Safety Assessment Principles

The TO2 technical observations which are applicable to the Safety Automation System (SAS) and the Process Automation System (PAS) are:

23. **T16.TO2.22** – The designer or future operator/licensee is requested to address the following points which have arisen from the review of the SAS/PAS CAE for SAP EDR.1 and update the CAE information:

    a. The CAE states that SIE QU633 provides a system level reliability study. However the study is not provided in SIE QU633.

       The designer or future operator/licensee is requested to update the CAE to demonstrate that SAS/PAS system level reliability study has been performed.

    b. The CAE claims that SIE QU 627 provides an FMEA of SPPA-T2000 based C&I systems (i.e. SAS, PAS and PICS). However, SIE QU 627 is the reliability analysis of the SPPA-T2000 platform and the document does not contain an FMEA.

       The designer or future operator/licensee is requested to update the CAE to demonstrate that an FMEA of the SPPA-T2000 has been performed.

24. **T16.TO2.23** - The designer or future operator/licensee is requested to address the following point which has arisen from the review of the SAS/PAS CAE for SAP EDR.2, and update the CAE information:

    The CAE claims that SIE QU 627 provides a reliability analysis for the SPPA-T2000 based C&I systems, i.e. SAS and PAS. However, the analysis addresses hardware only and does not take into account systematic software failures of the application software.

    The designer or future operator/licensee is requested to update the CAE to provide evidence of a reliability analysis for the SPPA-T2000 based C&I systems, i.e. SAS and PAS that includes consideration of systematic software failures.

25. **T16.TO2.24** - The designer or future operator/licensee is requested to address the following points which have arisen from the review of the SAS/PAS CAE for SAP EDR.3, and update the CAE information:

    a. The CCF analysis only applies to the SAS (not PAS).

Annex 6

The designer or future operator/licensee is requested to update the CAE to demonstrate that a CCF analysis of the PAS has been performed.

b. The analysis only addresses digital aspects of the SAS system, and there is no reference to an analysis of Common Cause Failure of non digital aspects of the system (e.g. electrical power.) Further evidence is needed to confirm that an adequate Common Cause Failure analysis has been performed on non digital aspects of the system.

The designer or future operator/licensee is requested to update the CAE to demonstrate that an adequate Common Cause Failure analysis has been performed on non digital aspects of the SAS system.

26. **T16.T02.25** - The designer or future operator/licensee is requested to address the following point has arisen from the review of the SAS/PAS CAE for SAP EQU.1, and update the CAE information:

The quality plan for SPPA based systems does not address qualification, as required by IEC 61513:2001, clause 6.4, and RCC-E chapter C5800.

The designer or future operator/licensee is requested to update the CAE to demonstrate that the requirements for qualification, as specified by IEC 61513:2001 clause 6.4, and RCC-E chapter C5800 are satisfied.

27. **T16.T02.26** - The designer or future operator/licensee is requested to address the following points which have arisen from the review of the SAS/PAS CAE for SAP EMT.7, and update the CAE information:

a. QU633 describes the periodic test between SICS and PAS/SAS at a high level of abstraction at the platform level. However, there is insufficient provided evidence to demonstrate how overlapping periodic test and self test ensures that the functionality of the complete safety-related function from sensor to actuator is provided.

The designer or future operator/licensee is requested to update the CAE to demonstrate that overlapping periodic test and self test ensures that the functionality of the complete safety-related function from sensor to actuator is tested.

b. Observation O14 from the HSE/NII Step 3 assessment requested a description of how SAP EMT.7 is satisfied for "F2 C&I not in continuous operation". This has not been addressed in the CAE information.

The designer or future operator/licensee is requested to update the CAE to demonstrate how SAP EMT.7 is satisfied for "F2 C&I not in continuous operation".

c. It is noted that the argument states '*For SAS, PAS and PICS Overlapping periodic testing and self-testing ensure that the functionality of the complete system (and its components) from sensor to actuator is provided.'*. However, the evidence does not address the PICS.

The designer or future operator/licensee is requested to update the CAE to demonstrate that overlapping periodic testing and self-testing ensure that the functionality of the PICS is provided.

28. **T16.T02.27** - The designer or future operator/licensee is requested to address the following point which has arisen from the review of the SAS/PAS CAE for SAP ESR.5, and update the CAE information:

Annex 6

The referenced evidence, DN 2.2.24, is specific to SAS. Confirmation is required that corresponding information is established for the PAS.

The designer or future operator/licensee is requested to update the CAE to confirm that DN 2.2.24 is applicable to the PAS, or if not, to update the CAE to demonstrate that the PAS is compliant with IEC 61513 and 62138

29. **T16.T02.28** - Evidence has been sought, from the Areva and Siemens quality plans (NLF-F DC 82 Rev C, PD110, Issue 1.0), to confirm that the requirements of IEC 61513:2001 are satisfied for Class 2 and 3 systems. For some clauses the provided evidence does not provide this confirmation.

    The designer or future operator/licensee is requested to demonstrate that the following requirements are satisfied:

    a. 6.1.2 *System Specification* - both quality plans state that this is beyond their scope.
    b. 6.1.6 *System Installation* - NLF-F DC 82 states that it is applied but also states that it is not addressed by this plan.
    c. For each of the following sub-clauses NLF-F DC 82 states that the clause is applied, but does not provide or refer to supporting evidence:
        - 6.2.5 - *System Installation Plan*
        - 6.2.6 - *System Operation Plan*
        - 6.2.7 - *System Maintenance Plan*
    d. Clause 6.4 – *Qualification* - both documents state that the clause is applied, but do not provide or refer to supporting evidence.

30. **T16.T02.29** - Evidence has been sought, from System Specification File SY710 to confirm that the requirements of IEC 62138:2004 Clauses 5.3 and 6.3 *Software Requirements* Specification are satisfied. It can be seen that the document does address the requirements of the clauses, however it includes requirements for the SPPA T2000 Platform and the SAS application.

    The designer or future operator/licensee is requested to indicate which aspects of System *Specification* File SY710 are applicable to each of the platform and the SAS application.

31. **T16.T02.30** - Evidence has been sought, from the Areva and Siemens quality plans (NLF-F DC 82 Rev C, PD110, Issue 1.0), to confirm that the requirements of IEC 62138:2004, Clause 5.8 & 6.8 – *Installation of Software on Site* is satisfied for Class 2 and 3 systems.

    NLF-F DC 82 states that the clause is applied, but does not provide or refer to supporting evidence.

    The designer or future operator/licensee is requested to demonstrate that the above clause is satisfied.

32. **T16.T02.31** - No evidence on the application of IEC 60987:2007 to the SPPA T2000 applications has been provided.

Annex 6

The designer or future operator/licensee is requested to demonstrate that the requirements of IEC 60987:2007 have been satisfied for SPPA-T2000 based systems on UK EPR.

The TO2 observation which is applicable to the Safety Information and Control System (SICS) is:

33. **T16.TO2.32** - The designer or future operator/licensee is requested to demonstrate that the following standards have been satisfied in the development and production of the Safety Information and Control System.
    - IEC 61513:2001
    - IEC 60987:2007
    - IEC 60780:1998

Conclusion of Task Review

For the PS, based on the sampled evidence, and subject to satisfactory resolution of the technical observations, there is no evidence to indicate that the requirements of relevant standards are not satisfied. There is some evidence of independent confidence building measures for the PS, however some areas for improvement have been identified.

For the NCSS and QDS, a demonstration of safety has not been provided.

For the SAS and PAS, based on the sampled evidence, and subject to satisfactory resolution of the technical observations, there is no evidence to indicate that requirements of relevant standards are not satisfied.

For the SICS, the review was limited to confirming that the equipment has been developed and qualified to appropriate nuclear hardware standards. This limited review is justified on the fact that the SICS is based on conventional technology i.e. it consists of a set of conventional controls and displays (push buttons, light indicators, analogue displays, recorders etc.). Insufficient information has been provided in the period of this review for it to be confirmed that the SICS has been developed and qualified to appropriate standards.

Annex 7

Review of the C&I Architecture for Safety Capability – TSC Summary[10]

Note this information has been imported from a TSC report (Ref. 32) and the formatting of the TSC report has been retained.

[10] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 7

A Annex: TSC Task Summary: Review of the C&I Architecture for safety capability

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of the C&I Architecture for safety capability (TSC Task 17) for the UK EPR reactor design.

This review follows on from the review of architecture-related claims and argumentation carried out in a preliminary activity (TSC Task 7), relating to:

a) defence in depth and failure mode management including common cause failure.
b) independence and diversity;
c) provision for automatic and manual safety actuation;
d) appropriateness of equipment type/class.

The aim of the review has been to gain confidence that the Requesting Party (EDF Energy and Areva NP, hereafter referred to as EDF and AREVA) has adequate evidence to support these architecture-related claims and argumentation. The review has included consideration of evidence to support further claims and argumentation presented by EDF and AREVA relating to conformance of the C&I architecture to 19 selected Safety Assessment Principles (SAPs). The review has taken due cognisance of selected HSE Technical Assessment Guidelines (TAGs) and international nuclear safety standards. The task has reviewed architecture-related evidence presented by EDF and AREVA via:

- the claims-argument-evidence table that provides the basis of the demonstration of SAP conformance;
- responses to Technical Queries;
- responses to actions from meetings involving EDF and AREVA, HSE/NII and the TSC;
- and responses to technical observations raised during Step 3, including architecture-related observations in the HSE/NII GDA Step 2 and Step 3 reports.

In addition, the task has reviewed changes to the UK EPR C&I architecture that have occurred since the end of Step 3 of the GDA process.

The scope of the evidence that is specific to UK EPR is defined by EDF and AREVA in *"UK EPR CONTROL AND INSTRUMENTATION (C&I) – SCOPE OF GDA"* (letter ND(NII)EPR00686N). The structures, systems and components (SSCs) that comprise the C&I architecture is consistent with this scoping letter. The main SSCs that were reviewed in the architecture review are as follows: Teleperm XS platform and its hosted systems (Protection System, Reactor Control, Surveillance and Limitation System, and Severe Accident I&C system); SPPA-T2000 platform and its hosted systems (Safety Automation System, RRC-B Safety Automation System, Process Automation System, and Process Information and Control System); Safety Information and Control System; Priority and Actuation Control System; Process Instrumentation Preprocessing System; class 1 network; class 2 network (SAS bus); and class 3 networks (Plant bus and Terminal bus). In addition, two further SSCs have been added to the C&I architecture in response to Regulatory Issue RI-UKEPR-002 – the Non-Computerised Safety System and the class 1 displays and controls interface with the Protection System – but evidence relating to these additional SSCs has not been developed in the timeframe of this review.

The C&I architecture has been modified significantly since the definition that was presented by EDF and AREVA in the April 2008 version of the Pre-Construction Safety Report (PCSR): The addition of the Non-Computerised Safety System has resulted in reduced reliability claims for the primary and secondary protection systems; several systems now have higher classification; a new class 2 network has been introduced for use by the secondary protection system; a new system has been added to

Annex 7

respond to certain types of severe accident; the interfaces with the Protection System have been changed so as to avoid inputs from lower-classified systems; class 1 controls and displays have been introduced in the Main Control Room and the Remote Shutdown Station.

A total of 27 technical observations resulting from the Task 17 review remain unresolved at the end of the review period. These observations have been designated as TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher – 8 of these observations have been designated as TO1 and 19 of these observations have been designated as TO2. Note that where a gap in the numbering sequence exists, this is due to the resolution of an observation that had been allocated this number.

Technical Observations designated TO1

The eight TO1 technical observations are as follows:

T17.TO1.01 - The categorisation and classification scheme in NEPS-F DC 557 does not conform to IEC 61226:2009 and UK expectations. The designer or future operator/licensee is requested to:

a. update the categorisation and classification scheme (eg. as defined in NEPS-F DC 557) with all appropriate IEC 61226:2009 clauses and use this to re-classify the C&I systems.

b. state explicitly the claim limits for each class in the categorisation and classification scheme so as to reflect the following:
For non-computer based systems, including systems with complex electronics such as Complex Programmable Logic Devices[11]:
- Class 1 1E-5 ≤ probability-of-failure-on-demand (pfd) < 1E-3
- Class 2 1E-3 ≤ pfd < 1E-2
- Class 3 1E-2 ≤ pfd ≤ 1E-1

For computer-based systems:
- Class 1 1E-4 ≤ pfd < 1E-2
- Class 2 1E-2 ≤ pfd
- Class 3 1E-1 ≤ pfd

For high demand or continuous modes of operation then the pfd is replaced by a frequency (f) of failure per year but the figures remain the same.

c. identify how the time following each fault at which, or the period throughout which, the main and diverse lines of defence will be called upon to operate, is taken into account in the classification and categorisation scheme.

T17.TO1.02 - With regard to the Fault Schedule in PEPR-F DC 4 rev B, the designer or future operator/licensee is requested to:

a. update the Fault Schedule to identify the C&I systems that are involved in each safety function.

[11] ND note: Depending on the degree of complexity, and the use of software techniques and tools the computer-based system limits may need to be applied.

Annex 7

b. confirm that the Fault Schedule is consistent with the Probabilistic Safety Assessment in its identification of all diverse lines of defence needed to meet the required risk mitigations, especially for infrequent events with high consequence.

Document ECECC080669 rev B "*Architecture of instrumentation and control system EPR FA 3: design principles and defence-in-depth*" states that the allocation of RRC-A functions is performed on a case-by-case basis, taking into account independence requirements (of the C&I system providing the defence from the initiating event). However, it was not possible to locate any results of this case-by-case analysis that shows that in all cases, each C&I safety and safety-related system is independent of, and invulnerable to, any fault that the system is claimed to act against. The designer or future operator/licensee is requested to:

c. substantiate the claim that each C&I safety and safety-related system is independent of, and invulnerable to, any fault that the system is claimed to act against.

T17.TO1.04 - The designer or future operator/licensee is requested to update the specification of the Protection System for UK EPR (NLN-F DC 193 rev A) to include the commitments to avoid networked (hardwired connections justified on a case-by-case basis) communication into the Protection System from lower classified systems.

T17.TO1.11 - The designer or future operator/licensee is requested to update the pre-construction safety report and identified references to:

a. capture the claims-argument-evidence information in PELL-F DC 9;

b. include the modifications to the architecture for UK EPR that have been committed to since November 2009. The update to include all commitments captured in the following documents:
   i. letter EPR00180R;
   ii. letter EPR00607N;
   iii. response to TQ-EPR-1003.

T17.TO1.14 - The designer or future operator/licensee is requested to update the pre-construction safety report to define the controls and displays to be provided by the class 1 extension to the Process Information and Control System, in the Main Control Room and in the Remote Shutdown Station, including whether the implementation of this class 1 extension will use the Qualified Display System or not.

T17.TO1.15 - The designer or future operator/licensee is requested to update the pre-construction safety report, and supporting documents such as "*Sizing of SICS*" (document ECEF021068 rev C), to ensure an adequate scope of parameters are defined for display using Class 1 equipment (e.g. by comparison with the category 1 safety parameters as defined by U.S. NRC Regulatory Guide 1.97 Revision 3 - May 1983). The designer or future operator/licensee is also requested to investigate the practicability of using a class 1 origin instead of a lower class origin for such safety parameters (when this is available).

T17.TO1.24 - The technology to be used for the implementation of the Non-Computerised Safety System is declared by EDF and AREVA to be out of scope of Step 4 of GDA, and as a result, its impact on the C&I architecture, and justification of its reliability claim, could not be reviewed. The designer or

Annex 7

future operator/licensee is requested to address this by provision of a safety demonstration through a Basis of Safety Case for the NCSS, when the supplier and technology for NCSS have been selected.

T17.TO1.25 - The designer or future operator/licensee is requested to incorporate the commitment made in letter EPR00180R into the safety case submission, regarding the disconnection of the Teleperm XS Service Unit during plant operation, to mitigate the risk that it could cause unintended interference to the operation of the class 1 part of the Protection System.

Technical Observations designated TO2

The nineteen TO2 technical observations are as follows:

T17.TO2.03 - The designer or future operator/licensee is requested to address the results of its review of the use of class 3 systems in the diverse line of defence for category A functions.

T17.TO2.05 - The designer or future operator/licensee is requested to address the following areas for improvement regarding the self-test function of Teleperm XS:

a. If there is repeated cycle overrun by the software application and/or service task, which causes the self-test function not to execute, this may not be detected for one hour before an alarm is raised. The designer or future operator/licensee is requested to substantiate the claim that safety is not compromised if the self-tests do not execute for one hour.

b. Table 1 in "*TXS Self-monitoring and fail-safe behaviour*" (document NLTC-G 2008 EN 0079 rev B) identifies some components that are not self-tested during cyclic operation without providing justification. The designer or future operator/licensee is requested to identify the full set of Teleperm XS platform components used by the Protection System that are not subject to self-test, and to justify why this does not compromise safety.

T17.TO2.06 - The designer or future operator/licensee is requested to address the following areas for improvement regarding the self-test function of the SPPA-T2000 platform:

a. to ensure that the fail-safe states of the SPPA-T2000 modules analysed in "*Self test coverage analysis*" (document SIE QU633 v5.0) are well-defined and documented.

b. to demonstrate full coverage of the SPPA-T2000 modules/components by self-test, and the justification for any absence of self-test.

c. to address the effects on safety of application software or service unit processing overrun that denies execution of the self-test software.

T17.TO2.07 - The designer or future operator/licensee is requested to ensure that Failure Modes and Effects Analyses have been completed for class 1 C&I components and systems, in particular:

a. Process Instrumentation Preprocessing System

b. Priority and Actuation Control System (PACS), plus addressing the results of the Reliability study for the actuation equipment for the Flamanville 3 reactor (FA3), including the PACS switchgear, due mid 2011. If the FA3 study is not directly applicable to the UK EPR then an appropriate reliability study should be completed for the UK EPR.

Annex 7

c. Reactor Trip equipment, including trip breakers and trip contactors.

T17.TO2.08 - The designer or future operator/licensee is requested to demonstrate the single failure criterion via functional and/or system-level redundancy for the class 1 Safety Information and Control System (SICS) controls/displays, and class 1 Priority and Actuation Control System/actuator (PACS) equipment, in particular for the following cases:

a. for SICS equipment that is shared across all four divisions, for example, the equipment that issues an order that is distributed to all four divisions;

b. for PACS/actuator equipment that is shared by multiple lines of defence for the same Postulated Initiating Event.

T17.TO2.09 - The designer or future operator/licensee is requested to demonstrate the single failure criterion for:

a. a single failure that disables an entire division performing an Engineered Safeguard Action function, such as a loss of common power supply at division level, when the function is implemented in only two divisions, and when the other instance of the Engineered Safeguard Action function is disabled due to maintenance.

b. consequential failures of C&I systems and their supporting equipment (cabinets, power, networks etc), as required by SAP EDR.4 paragraph 175.

T17.TO2.10 - The designer or future operator/licensee is requested to justify the allocation of manual actuation over automatic actuation for each safety and safety-related I&C function for UK EPR.

T17.TO2.13 - The selection of the technology and supplier for the Turbine Control system for UK EPR is out of scope of Step 4 of GDA. The designer or future operator/licensee is requested to ensure a safety demonstration is produced for the Turbine Control system when the supplier and technology have been selected.

T17.TO2.16 - The designer or future operator/licensee is requested to demonstrate that the manual controls in the Remote Shutdown Station, and the Terminal Bus, will be usable when the Main Control Room becomes uninhabitable. In particular, a response from EDF and AREVA has stated that a design study is in progress for the Flamanville 3 reactor, to address a technical solution for avoiding spurious commands being sent from the operator workstation in the Main Control Room whilst uninhabitable, potentially causing overload of the Terminal Bus (which may disable the operator workstation in the Remote Shutdown Station). The designer or future operator/licensee is requested to address the results of this study for UK EPR.

T17.TO2.17 - The designer or future operator/licensee is requested to update the safety case submission to record which Protection System functions use internal diverse detection, and which do not, and for those that do not, to include the justifications.

T17.TO2.18 - The review of the adequacy of the frequency of periodic testing of class 1 equipment is out of scope for Step 4 of GDA. The designer or future operator/licensee is requested to update the safety demonstration to include this information.

Annex 7

T17.TO2.19 - The designer or future operator/licensee is requested to demonstrate the adequacy of the monitoring of class 1 actuators used by the Protection System and by category A Safety Information and Control System functions.

T17.TO2.20 - The review of the Operating Technical Specification for each C&I system to examine whether it defines either a grace period for repair or a fail-safe operating mode, and to examine if the grace period is exceeded, whether a fail-safe action is required by the operator, is out of scope for Step 4 of GDA. The designer or future operator/licensee is requested to update the safety demonstration to include this information.

T17.TO2.21 - The adequacy of the controls provided by C&I systems to maintain variables within specified ranges, is out of scope of GDA. Likewise, the definition of Temporary Operating Modes that allow online modification of plant variables via the Service Unit is out of scope of GDA. The designer or future operator/licensee is requested to update the safety demonstration to include this information.

T17.TO2.22 - The design of communications systems that enable information and instructions to be transmitted between locations, and that provide external communications with auxiliary services and such other organisations as may be required, is out of scope of GDA. The designer or future operator/licensee is requested to update the safety demonstration to include this information.

T17.TO2.23 - Some types of external hazard are out of scope of GDA because they are site-dependent, and hence the risk assessment requires site-specific data. The designer or future operator/licensee is requested to update the safety demonstration to include this information.

T17.TO2.26 - Document ECECC100744 rev A “Plant I&C requirement specification” applicable to UK EPR does not contain the C&I functional requirements, and instead refers to a document that defines the classification scheme. The designer or future operator/licensee is requested to update the safety case submission to identify the set of C&I functional requirements.

T17.TO2.27 - The presentation by EDF and AREVA in response to action 43-I&C-6 states that the relay logic in the Priority and Actuation Control System always prioritises signals from the Protection System over signals from the Non Computerised Safety System (NCSS), and over signals from the SPPA-T2000 Safety Automation System (SAS), Process Automation System (PAS), and Process Information and Control System (PICS). The designer or future operator/licensee is requested to:

a. demonstrate that the effect of a fault in the Protection System that attempts to set "Protection Order On" when "Protection Order Off" is also set cannot inhibit or impede orders from NCSS, SAS, PAS or PICS;
b. demonstrate that it is never the case (or fully justify each case as being appropriate) that a Protection System signal that is part of a category B (or lower) function can cause a signal from SAS, PAS, PICS, or NCSS that is part of a category A function for the same actuator, to be inhibited or impeded, due to this prioritisation. The demonstration to include consideration of Protection System failures such that operation of any category A function by backup systems is not frustrated by such failures.

T17.TO2.28 - Within the Probabilistic Safety Assessment model, the Process instrumentation Preprocessing System (PIPS) is included in the sensor modelling, and the Priority and Actuation Control System (PACS) is included in the actuator modelling. The designer or future operator/licensee is requested to review the reasonable practicability of modelling the PIPS and PACS systems separately from the sensors and actuators, in order to make explicit:

Annex 7

a. the occurrence of any potential common cause failures in these systems and their modules;
b. the need for diversity if reliability claims for modules in these systems exceed acceptable limits.

A number of further observations that relate to the C&I architecture have arisen from the review of the responses to RI-UKEPR-002 and are documented in "*Review of Responses to Regulatory Issue RI-UKEPR-002 - Task 20*".

Conclusion of Task Review

With regard to the architecture-related observations in the HSE/NII GDA Step 3 report, the following conclusions are reached:

a) "*Protection systems reliability claims difficult if not impossible to substantiate*" has been resolved by the commitment in letter EPR00180R to reduce the reliability claims as a result of introduction of the Non-Computerised Safety System;
b) "*Independence between the safety (Class 1) and safety related systems (Class 2/3) appears to be significantly compromised*" has been resolved by changes to class 1 system interfaces with lower-classified systems;
c) "*No Class 1 manual controls or indications either in the Main Control Room or Remote Shutdown Station*" has been resolved by the class 1 extension to the Process Information and Control System;
d) "*EPR function categories / equipment class assignments do not appear to align with UK expectations as defined in BS IEC 61226:2005*" has been progressed and outstanding points are covered by technical observation T17.TO1.01 and potential GDA Issues PGI-UKEPR-C&I-02 and PGI-UKEPR-CC.01[12];
e) "*lack of overall specification of the C&I architecture*" has partially been resolved, and the outstanding point (absence of functional requirements for C&I) has been covered by technical observation T17.TO2.26;
f) "*absence of key information in the PCSR*" has been progressed and outstanding points are covered by technical observation T17.TO1.11 and potential GDA Issue PGI-UKEPR-C&I-04[13].

Of the 19 SAPs that have been reviewed by Task 17, only two (ESS.1 and ESS.2) have no associated technical observation. Nevertheless, in view of the fact that written commitments have been made by EDF and AREVA to resolve the topics in the identified TO1 observations, which have also been captured in the set of potential GDA Issues, it is the opinion of the TSC that an acceptable way forward has been achieved for the major architecture-related elements of the C&I design to meet the intent of the appropriate SAPs, TAGs and IEC standards.

[12] ND note: GI-UKEPR-CC-01 is the issued version of the provisional GDA Issues (pGI) that is addressing the concern identified here.

[13] ND note: GI-UKEPR-CI-03 is the issued version of the provisional GDA Issue (pGI).

Annex 8

Review of the Diversity of Those Systems Contributing to the Implementation of Category A Functions – TSC Summary[14]

Note this information has been imported from a TSC report (Ref. 33) and the formatting of the TSC report has been retained.

[14] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 8

A Annex: TSC Task Summary: Review of the diversity of those systems contributing to the implementation of category A functions

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of the diversity of those systems contributing to the implementation of category A functions (TSC Task 18) for the UK EPR reactor design.

The use of various forms of diversity within systems performing protection functions is important to minimise the risk of simultaneous failure on demand of those systems.

This review follows on from the review of diversity claims and argumentation carried out in a preliminary activity (TSC Task 8), relating to:

a) equipment diversity (including diversity of platform);
b) diversity of verification and validation;
c) diversity of physical location (segregation);
d) software diversity;
e) functional / data / signal diversity;
f) diversity of design / development;
g) diversity of specification.

The aim of the review has been to gain confidence that the Requesting Party (EDF Energy and Areva NP, hereafter referred to as EDF and AREVA) has adequate evidence to support these diversity claims and arguments. This has included review of the evidence to support further claims and argumentation presented by EDF and AREVA relating to the conformance of specific C&I protection systems to selected Safety Assessment Principles (SAPs) that relate to diversity.

Five SAPs have been considered during the review (EDR.2 - Redundancy, Diversity and Segregation, EDR.3 – Common Cause Failures, EDR.4 - Single Failure Criterion, ESS.18 - Failure Independence, and ERC.2 - Shutdown Systems). The review has taken due cognisance of selected HSE Technical Assessment Guides (TAGs) and international nuclear safety standards. The task has also reviewed evidence presented by EDF and AREVA via:

- the claims-argument-evidence table that provides the basis of the demonstration of SAP conformance;
- responses to Technical Queries;
- responses to actions from meetings involving EDF and AREVA, HSE/NII and the TSC;
- and responses to technical observations raised during the preliminary activity, including diversity-related observations in the HSE/NII GDA Step 2 and Step 3 reports.

In addition, the task has reviewed diversity-related changes to the UK EPR C&I architecture that have occurred since the end of Step 3 of the GDA process.

The scope of the evidence that is specific to UK EPR is defined by EDF and AREVA in *"UK EPR CONTROL AND INSTRUMENTATION (C&I) – SCOPE OF GDA"* (letter ND(NII)EPR00686N). The review of the diversity of those systems contributing to the implementation of category A functions is consistent with this scoping letter. The main systems that were reviewed in the diversity review are as follows: Protection System (hosted on the Teleperm XS platform); Safety Automation System and Process Automation System (hosted on the SPPA-T2000 platform); and the Non-Computerised Safety System

Annex 8

(NCSS), which has been added to the C&I architecture since Step 3 of GDA in response to Regulatory Issue RI-UKEPR-002.

A total of 11 technical observations resulting from the review remain unresolved at the end of the review period. These technical observations have been designated as TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher – 5 of these observations have been designated as TO1 and 6 of these observations have been designated as TO2. Note that where a gap in the numbering sequence exists, this is due to the resolution of an observation that had been allocated this number.

Technical Observations designated TO1

The five TO1 technical observations are:

T18.TO1.01 - The designer or future operator/licensee is requested to update the Pre-Construction Safety Report (PCSR) to capture the claims-argument-evidence information, and to reflect the diversity-related changes that result from the modifications to the architecture for UK EPR that have been committed to by EDF and AREVA since June 2009.

T18.TO1.02 - The designer or future operator/licensee is requested to provide detailed substantiation for the reliability claims and classification of all C&I components used by more than one system important to safety, and potentially by more than one line of defence, for example, common use of sensors, the Process instrumentation Preprocessing System, actuators, and the Priority and Actuator Control System, by the protection systems for the same Postulated Initiating Event. In addition:

a. the substantiation should consider the potential for common mode failure as a result of use of such common components;

b. where the required reliability of a device or system exceeds expected claim limits for this type of equipment, the designer or future operator/licensee is requested to present a solution that employs diversity to reduce the reliability claims within the claim limits.

T18.TO1.03 - The technology to be used for the implementation of the Non-Computerised Safety System is out of scope of GDA Step 4, and as a result, its diversity from that of the computerised platforms, and justification of its reliability claim, could not be assessed. The designer or future operator/licensee is requested to address this by provision of a safety demonstration through a Basis of Safety Case for the diversity aspects of the NCSS when the supplier and technology for NCSS have been selected.

T18.TO1.04 - Version S5 of the SPPA-T2000 platform is believed to be obsolete. Should a different version be selected for UK EPR, the designer or future operator/licensee is requested to substantiate the diversity claim between Teleperm XS and the new version. This substantiation to cover, amongst others, diversity of the technology (including hardware and software components, communication protocol, and supplier etc.) of the class 1 Profibus network in Teleperm XS, and the technology of the class 2 Profibus DP network in the AS 620B Automation System in the SPPA-T2000. The designer or future operator/licensee is also requested to present a full diversity analysis between the UK EPR version of SPPA-T2000 and the technology selected for the Non-Computerised Safety System.

T18.TO1.05 - The designer or future operator/licensee is requested to address in the safety case submission, the commitment in the response to Technical Query 368 observation 3 – "*Areva/EDF will*

Annex 8

avoid use of, for a given initiating event, the same type of smart equipment in multiple lines of defence."

Technical Observations designated TO2

The six TO2 technical observations are:

T18.TO2.01 - **The designer or future operator/licensee is requested to include in the safety case submission the analysis of the effect of the loss of one or more divisions on the Protection System (PS) category A functions that need to exchange information across all divisions, and to justify why this does not compromise the safety aspects of these category A functions.**

T18.TO2.03 - **The designer or future operator/licensee is requested to update the Fault Schedule to identify the C&I systems that are involved in each safety function, and the required risk reductions.**

T18.TO2.06 - **There are two independent mechanisms for shutdown – reactor trip and extra boration – and both are claimed to be actuated by the diverse protection systems Protection System (PS) and Safety Automation System (SAS). Whilst there is evidence that PS and SAS implement diverse Reactor Trip functions, the designer or future operator/licensee is requested to demonstrate adequate diversity and common mode failure analysis for:**

a. **the equipment used by PS to actuate boration, compared to the equipment used by SAS to actuate boration;**

b. **the equipment used by either PS or SAS to actuate reactor trip, compared to the equipment used by that system to actuate boration.**

T18.TO2.07 - **Document "*TELEPERM XS based systems - Concept for Electrical Separation*" (NLE-F DC 249 rev C) specifies the requirements and technological solutions for electrical separation between Teleperm XS equipment and other technology equipment for the Flamanville 3 reactor. For each solution, evidence is provided to demonstrate compliance with the appropriate clause in the French Nuclear Standard "*RCC-E*", except for two solutions in section 4.2, which are noted as temporary solutions, with RCC-E compliance being "under analysis". These relate to the electrical signals that are output from, or input to Teleperm XS computers, using an overvoltage barrier module to provide protection. The designer or future operator/licensee is requested to demonstrate for these two cases that a solution that complies with RCC-E has been designed for UK EPR.**

T18.TO2.08 - **SAP ERC.2 paragraph 445 relates to, for example, situations where the control rods fail to insert on a Reactor Trip signal from the Protection System. In this situation an Anticipated Transient Without Scram (ATWS) signal is initiated by the C&I to actuate the Extra Boration System (EBS) and Safety Injection System (SIS) to inject borated water. The designer or future operator/licensee is requested to address this scenario in the claims-argument-evidence entry for SAP ERC.2.**

T18.TO2.09 - **Regarding diversity of specification:**

a. **The requirements specifications of the Teleperm XS and the SPPA-T2000 platforms were not made available during the timescales of the review. Hence a diversity analysis of these specifications could not be carried out. The designer or future operator/licensee is requested**

Annex 8

to demonstrate adequate diversity in the method of specifying the requirements of Teleperm XS and SPPA-T2000.

b. The requirements for diverse systems such as the Protection System (PS) and the Safety Automation System (SAS) are each expressed using high-level function block diagrams. The designer or future operator/licensee is requested to demonstrate adequate diversity in the method of specifying the requirements of PS and SAS.

A number of further observations that relate to diversity aspects of the C&I architecture have arisen from the review of the responses to Regulatory Issue RI-UKEPR-002 and are documented in "*Review of Responses to Regulatory Issue RI-UKEPR-002 - Task 20*" - these observations are prefixed by "T20" and their significance is documented in the aforementioned Task 20 report. Reference is also made to observations raised by the review of C&I architecture that are documented in "*Step 4 Report for Task 17: Review of C&I Architecture for UK EPR*"– these observations are prefixed by "T17".

Conclusion of Task Review

With regard to the seven aspects of diversity that were covered by the review, the following conclusions are reached:

a) equipment diversity (including diversity of platform) – the most significant observation is for the designer or future operator/licensee to provide detailed substantiation for the reliability claims and classification of all C&I components used by more than one system important to safety, and potentially by more than one line of defence (T18.T01.02);
b) diversity of verification and validation – the most significant observation is for the designer or future operator/licensee to justify diversity between Teleperm XS and SPPA/T2000 on verification / validation tools, methods and teams (T20.A1.3.4 (T02));
c) diversity of physical location (segregation) – the most significant observation is for the designer or future operator/licensee to update the specification of the Protection System to include the commitments made by EDF and AREVA regarding inputs to the Protection System from lower class systems, and from the Teleperm XS Service Unit (T17.T01.04 and T17.T01.25);
d) software diversity – the most significant observation is for the designer or future operator/licensee to justify diversity between Teleperm XS and SPPA/T2000 on software development tools, methods and programming environment (T20.A1.3.4 (T02));
e) functional / data / signal diversity – the most significant observation is for the designer or future operator/licensee to provide detailed substantiation for the reliability claims and classification of sensors (including Smart sensors) and sensor conditioning modules used by more than one system important to safety, and potentially by more than one line of defence (T18.T01.02 and T18.T01.05);
f) diversity of design / development – the most significant observation is for the designer or future operator/licensee to justify diversity between Teleperm XS and SPPA/T2000 on design / development tools, methods and programming environment (T20.A1.3.4 (T02));
g) diversity of specification – observations were raised requesting the designer or future operator/licensee to demonstrate adequate diversity in the method of specifying the requirements of Teleperm XS compared to SPPA-T2000, and the requirements of the Protection System compared to the Safety Automation System (T18.T02.09).

A further conclusion is that there is the need to repeat aspects of these diversity reviews when the technology and supplier for the Non-Computerised Safety System has been selected (T18.T01.03), and when the version of the SPPA-T2000 platform for UK EPR has been finalised (T18.T01.04).

Annex 8

With regard to the four main diversity-related observations in the HSE/NII GDA Step 3 report, the following conclusions are reached:

a) "*excessive reliability claim for the diverse protection systems taken together*" has been resolved by the commitment in letter EPR00180R to reduce the reliability claims as a result of introduction of the Non-Computerised Safety System;
b) "*lack of evidence of platform diversity*" has been progressed and outstanding points are covered by the following observations: T20.A1.3.4 (TO2), T18.TO1.03, T18.TO1.04, and T18.TO2.09, and by potential GDA Issue PGI-UKEPR-C&I-07 action 1[15];
c) "*lack of evidence of diversity within systems in the same safety group when high reliability is needed*" has been progressed and outstanding points are covered by observation T18.TO1.02, and potential GDA Issue PGI-UKEPR-C&I-07 action 9[16];
d) "*absence of key information in the PCSR*" has been progressed and outstanding points are covered by observation T18.TO1.01, and potential GDA Issue PGI-UKEPR-C&I-04[17].

Of the five SAPs considered in the Task 18 review, all have associated technical observations. Nevertheless, the diversity-related changes that have been introduced into the C&I architecture since GDA Step 3 have resulted in each of these five SAPs being addressed in principle.

It is the opinion of the TSC that an acceptable way forward has been achieved for the major diversity-related elements of the C&I design to meet the intent of the appropriate SAPs, TAGs and IEC standards, subject to successful resolution of the observations arising from this review, and the applicable potential GDA Issues.

[15] ND note: GI-UKEPR-CI-06.A1 is the issued version of the provisional GDA Issue (pGI).

[16] ND note: GI-UKEPR-CI-06.A9 is the issued version of the provisional GDA Issue (pGI).

[17] ND note: GI-UKEPR-CI-03 is the issued version of the provisional GDA Issue (pGI).

Annex 9

Review of Responses to Regulatory Issue RI-UKEPR-002 – TSC Summary[18]

Note this information has been imported from a TSC report (Ref. 34) and the formatting of the TSC report has been retained.

[18] ND note: Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 9

A Annex: TSC Task Summary: Review of Responses to Regulatory Issue RI-UKEPR-002

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of the responses by EDF and AREVA to the actions in Regulatory Issue RI-UKEPR-002 (TSC Task 20) within the action plan defined in letter ND(NII) EPR00459R.

The Regulatory Issue RI-UKEPR-002 was closed by HSE/NII in November 2010 via letter EPR0700266N.

However there remain open technical observations from the TSC Task 20 review, some of which have been covered by actions within Potential GDA Issues that relate to C&I for UK EPR. This Annex lists the 19 open technical observations that resulted from the Task 20 review. Each technical observation has been identified throughout the Task 20 review period using a unique identifier that is of the form "*T20.<action number within RI-UKEPR-002>.<index>*". Each technical observation has also been designated as "*TO1*" or "*TO2*" by the TSC depending on its significance, of which TO1 is the higher. The Task 20 open technical observations are listed below, and have been grouped according to the subject matter of the following TSC Tasks:

a) TSC Task 14, which has reviewed the Quality Assurance arrangements and procedures that are defined by EDF-CNEN and Areva NP Quality Management Systems, and that relate to the lifecycle of class 1, 2 and 3 C&I systems;
b) TSC Task 15, which has reviewed the evidence to support the classification of the class 1 and 2 pre-developed components of the C&I architecture, in particular the Teleperm XS, and SPPA-T2000 platforms;
c) TSC Task 16, which has reviewed the evidence to support the classification of the class 1 and 2 C&I systems important to safety, in particular the Protection System and the Safety Automation System;
d) TSC Task 17, which has reviewed the C&I architecture for safety capability;
e) TSC Task 18, which has reviewed the evidence to support the diversity claims and argumentation of those C&I systems contributing to the implementation of category A functions.

Note that where a gap in the indexing sequence exists in the technical observation identifiers, this is due to the resolution of a technical observation that had been allocated this index during the Task 20 review period.

Applicable to all TSC Tasks

T20.A1.2.4 – designation TO1 - The selection of the supplier and technology to be used for the Non Computerised Safety System (NCSS) platform has not yet been made, and hence the review of the suitability of the technology, and of the lifecycle processes to develop class 2 NCSS application functions, to meet reliability claims, safety requirements and diversity criteria, has not been possible. The designer or future operator/licensee is requested to address this by provision of a safety demonstration through a Basis of Safety Case for the NCSS, when the supplier and technology for NCSS have been selected.

Annex 9

Task 15 (Pre-Developed Components)

T20.A1.4.1 – designation TO1 - **The designer or future operator/licensee is requested to:**

a) **justify the class 1 software reliability claim for Teleperm XS and the Protection System, based on the Production Excellence and Independent Confidence Building argument.**

b) **demonstrate compliance with IEC 60987 for the development, verification and qualification of the SPPA-T2000 platform hardware.**

c) **align the reliability claims for the Reactor Control, Surveillance and Limitation System, and the Severe Accident Instrumentation & Control System, that are defined by the Compact Model for the UK EPR PSA (section 4.2.1 of NEPS-F DC 576 rev A) with the claim limits for computer-based systems in observation T17.TO1.01, in particular:**

d) **- Class 2 1E-2 ≤ pfd**

e) **- Class 3 1E-1 ≤ pfd**

T20.A1.5.2 – designation TO1 - **The designer or future operator/licensee is requested to demonstrate compliance of Teleperm XS lifecycle processes with IEC 60880 and IEC 60987.**

T20.A1.5.5 – designation TO1 - **The designer or future operator/licensee is requested to justify the use of programmable complex electronic components within the Teleperm XS modules that are components of UK EPR class 1 systems. The justification should identify the standards, guidance and criteria that are used to demonstrate that the components are fit for purpose, and provide evidence of their application.**

Task 16 (Systems Important to Safety)

T20.A1.4.3 – designation TO2 - **The designer or future operator/licensee is requested to justify the differences between instances of the Protection System across the four divisions, and the argument for how this does not compromise redundancy or overall reliability.**

T20.A1.5.1 – designation TO1 - **The designer or future operator/licensee is requested to address the following areas for improvement that resulted from the review of production excellence and independent confidence building measures for the Protection System in document ENSECC090137 Rev B:**

a) **lack of mention of the use of formal methods, and the limitations of the PolySpace tool for static analysis (no formal proof capability);**

b) **the need for a detailed investigation into the reasonable practicability of increasing the number of statistical tests that are executed in the target environment from 5000 during the site licensing phase, and the need to provide a plan of all activities required to implement the statistical tests;**

c) **lack of mention of qualification of the development tool-chain for class 1 application development, and in particular, validation of the compiler.**

T20.A2.2.3 – designation TO2 – **The specification of the Protection System for UK EPR in document NLN-F DC 193 rev A contains a note that suggests that it does not fully reflect the UK EPR solution and that this specification will only be completed during the site license phase. The designer or future**

Annex 9

operator/licensee is requested to present a clear statement on the parts of the Protection System specification that are to be considered as complete for UK EPR, as documented in NLN-F DC 193 Rev A.

Task 17 (C&I Architecture)

T20.A1.3.5 – designation TO1 - The designer or future operator/licensee is requested to justify the reliability claims of the Priority and Actuator Control System and Reactor Trip equipment when either is shared by more than one line of defence for the same Postulated Initiating Event.

T20.A2.2.1 – designation TO1 - The designer or future operator/licensee is requested to address the following commitments made in the response to TQ-EPR-1003 regarding one-way communication from the Protection System to lower-classified systems:

a) Signal from Safety Automation System (SAS) / Process Automation System (PAS) to the Protection System (PS) for the periodic test of the Emergency Feed Water System pump (EFWP) – "*A solution to inhibit this signal when no periodic test is being performed will be implemented. The detailed solution will be defined during the detailed design phase (outside the scope of GDA)*".

b) For all signals from SAS/PAS to PS – "*A final confirmatory analysis, based on the final list of exchanged signals, will be performed during the detailed design phase outside the scope of GDA*."

c) "*The alarms from the Reactor Control, Surveillance and Limitation System to the Safety Information & Control System will be implemented by a separate connection without interface with the Protection System*."

d) "*A separate connection from the Severe Accident Instrumentation and Control System (SA I&C) to the Process Information & Control System will be implemented in the UK EPR in order to remove all connections from the SA I&C to the Protection System*."

e) "*...the TELEPERM XS gateway GW1 and the network to the Monitoring and Service Interface will be implemented with E1A TELEPERM XS components.*"

f) Analysis of hard-wired connections from the Non Computerised Safety System to PS.

It is noted that there may be detailed implementation issues which cannot be fully addressed under GDA.

T20.A2.3.2 – designation TO1 - The designer or future operator/licensee is requested to demonstrate non-interference in the operation of a higher class system by the operation of a lower class system, for all cases where C&I systems of different classification are connected and can operate as part of the same safety function. The demonstration to address communication from the class 3 Process Information & Control System (PICS), via class 3 networks, to the class 2 Safety Automation System (SAS).

T20.A2.3.4 – designation TO2 - The designer or future operator/licensee is requested to demonstrate that electrical separation is implemented for each I&C system hosted by the SPPA-T2000 platform.

Annex 9

T20.A3.6 – designation TO1 – EDF and AREVA has indicated in letter EPR00607N that the intention for UK EPR is to implement a class 1 Qualified Display System (QDS) for the class 1 displays and controls sent to the Protection System, in both the Main Control Room (MCR) and the Remote Shutdown Station (RSS). The designer or future operator/licensee is requested to:

a) produce detailed substantiation of the Class 1 control and display facilities in the MCR and RSS, noting the strong preference of HSE/NII for these to be the same for MCR and RSS, and for these to include manual Reactor Trip and Engineered Safeguard Action controls, as well as Permissives and Resets for the Protection System;

b) justify any class 1 controls and displays provided by the Safety Information & Control System (SICS) in the MCR, that are not supported by the QDS in the RSS, especially relating to SICS controls sent to the Safety Automation System and the Non Computerised Safety System;

c) produce a Basis of Safety Case for the Class 1 control and display system (QDS);

d) produce a justification in terms of the functional coverage of the QDS (the response to include consideration of US Nuclear Regulatory Commission Regulatory Guide 1.97 Revision 3).

T20.A4.6.2 – designation TO1 - The designer or future operator/licensee is requested to consider whether the Process Automation System (PAS) implements any of the main reactor controls, and if so, to justify why category B is not the appropriate categorisation of these functions, and why class 2 is not the appropriate classification of the PAS system.

T20.A5.4 – designation TO2 - The designer or future operator/licensee is requested to demonstrate that performance tests that verify end-to-end response times from sensor data acquisition through to sending an actuation order, have been executed without failure for the Protection System and Safety Automation System safety and safety-related functions on the Flamanville 3 reference implementation.

T20.A5.5 – designation TO2 - The designer or future operator/licensee is requested to demonstrate, for those functions important to safety which use the Class 3 Terminal bus and/or Plant bus, that end-to-end response time requirements are achievable by design.

Task 18 (Diversity)

T20.A1.2.3 – designation TO1 - The designer or future operator/licensee is requested to address the following review comments in a revision of the Non Computerised Safety System (NCSS) diversity requirements specification.

a) Please clarify how analysis of Common Cause Failure (CCF) as a result of shared sensors, or shared use of signal conditioning systems (PIPS), or shared use of actuators, by more than one of the protection systems, is taken into account in the Probabilistic Safety Assessment (PSA). In this context, note that the claim limit for hardware-based systems as defined by the SAPs and TAGs is 1E-5 pfd.

b) There are a number of entries where it is stated “no diversity requirement”. Please ensure that the reasons for there being no diversity requirement is explained and justified in the document. For example, it is necessary to ensure relevant IEC 61513 clauses are addressed (e.g. design and test diversity) and in particular the I&C system tests which are part of verification and validation would appear to require diversity.

Annex 9

c) Please clarify why there is no diversity requirement for the NCSS maintenance processes, particularly relating to outage maintenance.

d) Please clarify whether diversity level Ed=3 / Hd=3 applies to the V&V for the NCSS platform (compared to that of the Teleperm XS and SPPA-T2000 platforms) and if so, to reflect this in the document. Also please clarify the role of third party certification organisations such as TÜV.

e) Please explain why the risk of error introduction by the use of common testing tools and/or a common test environment between NCSS and the Protection System (or Safety Automation System) is not a concern.

f) Please explain how the risk of CCF due to the use of common basic components (such as capacitors and resistors) is addressed and factored into the PSA.

T20.A1.3.1 – designation TO1 - The designer or future operator/licensee is requested to:

a) substantiate the probabilistic claims for any sensor, and any module of the sensor conditioning and decoupling system (PIPS), that is used by more than one system important to safety, and potentially by more than one line of defence. Where probabilistic claims exceed claim limits for such devices that are defined by HSE/NII, the designer or future operator/licensee is requested to present a solution that employs diversity to reduce the reliability claims within the claim limits.

b) align the reliability claim for non-class-1 instrumentation in the UK EPR PSA, as given in the Compact Model (section 4.1 of document NEPS-F DC 576 rev A), with the claim limits stated in observation T17.TO1.01b, in particular:

c) - Class 2 1E-3 ≤ pfd < 1E-2

d) - Class 3 1E-2 ≤ pfd ≤ 1E-1.

T20.A1.3.4 – designation TO2 - The designer or future operator/licensee is requested to justify diversity between Teleperm XS and SPPA-T2000 platforms, on tools, methods and programming environment. This is also to address independence of Teleperm XS and SPPA-T2000 teams.

T20.A1.4.2 – designation TO1 - The designer or future operator/licensee is requested to demonstrate the reliability of the protection systems when taken in combination. If multiplication of probability-of-failure-on-demand values is used, then the adequacy of independence and diversity needs to be established.

Conclusion of Task Review

Although Regulatory Issue RI-UKEPR-002 has been closed, the designer or future operator/licensee is requested to respond to the technical observations resulting from the Task 20 review. It is noted that in some cases, this may be achieved via resolution of actions in the Potential GDA Issues raised by HSE/NII that relate to C&I.